

Finiteness properties of affine difference algebraic groups

Michael Wibmer*

December 3, 2019

Abstract

We establish several finiteness properties of groups defined by algebraic difference equations. One of our main results is that a subgroup of the general linear group defined by possibly infinitely many algebraic difference equations in the matrix entries can indeed be defined by finitely many such equations. As an application, we show that the difference ideal of all difference algebraic relations among the solutions of a linear differential equation is finitely generated.

Introduction

Similar to the case of affine algebraic groups, affine difference algebraic groups can be realized as subgroups of general linear groups. However, the defining equations here are not simply polynomials in the matrix entries but difference polynomials, i.e., the defining equations involve a formal symbol σ that has to be interpreted as a ring endomorphism. For example, if G is the difference algebraic subgroup of GL_n defined by the algebraic difference equations $X\sigma(X)^T = \sigma(X)^T X = I_n$ and $\sigma: \mathbb{C} \rightarrow \mathbb{C}$ is the complex conjugation map, then $G(\mathbb{C}, \sigma)$ is the group of all complex unitary $n \times n$ -matrices.

Alternatively, affine difference algebraic groups can be described as affine group schemes with a certain additional structure (the difference structure). As schemes, they are typically not of finite type, but they enjoy a certain finiteness property with respect to the difference structure; they are “of finite σ -type”.

A difference field is a field equipped with an endomorphism σ , a classical example is $\mathbb{C}(x)$ with $\sigma(f(x)) = f(x+1)$. From an algebraic point of view, an affine difference algebraic group G over a difference field k corresponds to a finitely σ -generated k - σ -Hopf algebra, i.e., a Hopf algebra $k\{G\}$ over k together with a ring endomorphism $\sigma: k\{G\} \rightarrow k\{G\}$ that extends $\sigma: k \rightarrow k$. The structure maps of the Hopf algebra are required to commute with σ , and $k\{G\}$ is required to be finitely σ -generated over k , i.e., there exists a finite set $B \subseteq k\{G\}$ such that $B, \sigma(B), \sigma^2(B), \dots$ generates $k\{G\}$ as a k -algebra. A difference ideal $\mathfrak{a}$ of $k\{G\}$ (i.e., an ideal of $k\{G\}$ with $\sigma(\mathfrak{a}) \subseteq \mathfrak{a}$) is called finitely σ -generated if there exists a finite subset F of $\mathfrak{a}$ such

*The author was supported by the NSF grants DMS-1760212, DMS-1760413, DMS-1760448 and the Lise Meitner grant M-2582-N32 of the Austrian Science Fund FWF.

Mathematics Subject Classification Codes: 12H10, 16T05, 14L15, 14L17. *Key words and phrases:* difference algebraic groups, difference algebraic geometry, difference Hopf algebras, differential Galois theory, difference algebraic relations.

that $F, \sigma(F), \sigma^2(F), \dots$ generates $\mathfrak{a}$ as an ideal. For clarity, we state here our main finiteness results in the language of Hopf algebras.

Theorem A. *Let $k\{G\}$ be a finitely σ -generated k - σ -Hopf algebra. Then,*

- (i) *every difference ideal of $k\{G\}$ that is a Hopf ideal is finitely σ -generated,*
- (ii) *every k - σ -Hopf subalgebra of $k\{G\}$ is finitely σ -generated,*
- (iii) *there are only finitely many minimal prime difference ideals in $k\{G\}$.*

In fact, we prove a very useful stronger version of (i). For a difference algebraic subgroup G of GL_n , this stronger version takes the following form: For $i \gg 0$ the ideal $\mathbb{I}(G)[i]$ of all difference polynomials in the matrix entries of order at most i that vanish on G , is generated by $\mathbb{I}(G)[i-1]$ and $\sigma(\mathbb{I}(G)[i-1])$.

A difference ideal in a finitely σ -generated k - σ -algebra need not be finitely σ -generated. A well-known counterexample is the difference ideal generated by $y\sigma(y), y\sigma^2(y), \dots$. The classical basis theorem in difference algebra ([Lev08, Theorem 2.5.11]) only applies to so-called perfect difference ideals: Every ascending chain of perfect difference ideals in a finitely σ -generated k - σ -algebra is finite. Recall that a difference ideal $\mathfrak{a}$ is perfect if $f\sigma(f) \in \mathfrak{a}$ implies $f \in \mathfrak{a}$. An interesting generalization of the classical basis theorem was suggested by E. Hrushovski in his seminal work [Hru04]:

Conjecture B. *Every ascending chain of radical well-mixed difference ideals in a finitely σ -generated k - σ -algebra is finite.*

Recall that a difference ideal $\mathfrak{a}$ is well-mixed if $fg \in \mathfrak{a}$ implies $f\sigma(g) \in \mathfrak{a}$. In [Lev15] it is shown that the above conjecture fails if the assumption that the ideals are radical is dropped. On the positive side, E. Hrushovski proved the conjecture under certain addition assumptions ([Hru04, Lemma 4.35]). Moreover, the conjecture (appropriately reformulated) has been proved for monomial and binomial difference ideals ([Wan17], [Wan18]).

We show that the Conjecture B is equivalent to: Every finitely σ -generated k - σ -algebra has only finitely many minimal prime difference ideals. Thus, point (iii) of Theorem A can be seen as providing another positive special case of Conjecture B.

Difference algebraic groups are the discrete analog of differential algebraic groups, i.e., groups defined by algebraic differential equations. Differential algebraic groups have always played an important role in differential algebra (see, e.g., [Cas72], [Sit75], [Cas75], [Cas78], [Kol85], [Cas89], [Bui92], [Bui93]) and are also presently an active area (see, e.g., [Pil97], [KP00], [Ovc09], [CS11], [MO11], [Kam13], [MO13], [Fre15], [Min15], [Pil17], [MO19], [CP].) See also [Mal10] for a more geometric approach to differential algebraic groups and [Bui98] for an arithmetic analog of difference/differential algebraic groups. Moreover, Galois theories for differential or difference equations where the Galois groups are differential algebraic groups ([Pil98], [Lan08], [CS07], [HS08]) have recently given a new impetus to the study of differential algebraic groups (see, e.g., [MOS15], [MOS14], [GO14], [HMO17]).

In contrast to the situation in differential algebra, difference algebraic groups have long played no role at all in difference algebra. The author can only speculate why. One reason might be that the traditional definition of a difference variety (see [Coh65, Chapter 4]) is not practical for studying groups.

Around the turn of the century a considerable interest in the model theory of difference fields emerged. (See e.g., [Mac97], [CH99], [CHP02].) Groups definable in ACFA, the model companion of the theory of difference fields, played a crucial role in remarkable applications of model theory to number theory, especially regarding the Manin-Mumford conjecture. See [Hru01], [Bou02], [Cha01], [Cha97], [Sca05], [Sca06], [SV99], [KP07]. Groups definable in ACFA have further been studied in [KP02] and [CH17].

Categories of representations of affine difference algebraic groups have been studied in [Kam13] and [OW17]. A cohomology theory for such representations and more general actions has been developed in [CK18]. Furthermore, torsors for affine difference algebraic groups are studied in [BW].

Understanding the relations among the solutions of a given linear differential equation is a classical and important problem. Often the interesting relations among the solutions are not simply algebraic relations but involve transformations of the variable or the parameters of the differential equation. For example, consider Bessel's differential equation

$$x^2 y'' + xy' + (x^2 - \alpha^2)y = 0.$$

The solution $J_\alpha(x)$, the Bessel function of the first kind, satisfies the well-known linear recurrence relation

$$xJ_{\alpha+2}(x) - 2(\alpha + 1)J_{\alpha+1}(x) + xJ_\alpha(x) = 0.$$

This is a *difference algebraic relation* with respect to the transformation $\alpha \mapsto \alpha + 1$ on the parameter α . Many classical functional identities can be interpreted as difference algebraic relations among solutions of linear differential equations. For example, the relation

$$\cos(2x) = 2\cos^2(x) - 1$$

is a *difference algebraic relation* with respect to the transformation $x \mapsto 2x$ on the variable x , satisfied by the solution $\cos(x)$ of $y'' + y = 0$.

A Galois theory for linear differential equations that is able to handle this kind of difference algebraic relations has been introduced in [DVHW14]. There is also a similar Galois theory for linear difference equations ([OW15]). The Galois groups in these Galois theories are affine difference algebraic groups and they measure the difference algebraic relations among the solutions.

Based on this Galois theory, we will show, as an application of point (i) of Theorem A, that, for a given linear differential equation, there exists a *finite* set F of difference algebraic relations among the solutions such that any other difference algebraic relation is a consequence of the difference algebraic relations in F . Or, formulated more algebraically, we show that the difference ideal of all difference algebraic relations among the solutions of a linear differential equation is finitely generated.

As illustrated in [DVHW17] and [OW15], the Galois theories described above make it possible to use structure results about affine difference algebraic groups to analyze and classify the possible difference algebraic relations among the solutions of certain linear differential and difference equations. In this respect, the understanding of the Zariski dense difference algebraic subgroups of a given affine algebraic group is highly relevant. For example, some understanding

of the Zariski dense difference closed subgroups of SL_2 , originating from [CHP02], is a key ingredient in proving that any two linearly independent solutions of the Airy equation are difference algebraically independent ([DVHW17, Corollary 6.10]).

Despite the recent works on difference algebraic groups and their applications to other areas outlined above, the theory of difference algebraic groups is still in its infancy and far from a level comparable to the state of the art of the theory of differential algebraic groups. The purpose of this article is therefore also to lay the groundwork for a further comprehensive study of affine difference algebraic groups¹. In particular, we introduce three basic numerical invariants for affine difference algebraic groups: the difference dimension, the order and the limit degree. These are in fact the three standard numerical invariants in difference algebra. However, in the standard textbooks [Coh65] and [Lev08] these are defined in terms of extensions of difference fields and it is not obvious how to generalize the definitions to difference Hopf algebras. Moreover, we establish a dimension theorem for affine difference algebraic groups: If H_1 and H_2 are difference algebraic subgroups of an affine difference algebraic group G , then $\sigma\text{-dim}(H_1 \cap H_2) \geq \sigma\text{-dim}(H_1) + \sigma\text{-dim}(H_2) - \sigma\text{-dim}(G)$. Interestingly, a similar statement fails for arbitrary difference varieties ([Coh65, Chapter 8, Section 8]). In regards to further developments in the theory of affine difference algebraic groups, we note that (ii) of Theorem A is crucial for establishing the existence of quotients (by normal subgroups) in the category of affine difference algebraic groups.

We conclude this introduction with an outline of the article: In Section 1 we recall the necessary definitions from difference algebra and difference algebraic geometry. Then, in Section 2 we introduce affine difference algebraic groups, present several examples and show that every affine difference algebraic group is isomorphic to a difference algebraic subgroup of some general linear group. Section 3 is the technical heart of this article. We show that the growth of the Zariski closures of a difference algebraic subgroup G of an affine algebraic group is governed by an algebraic group that we term the *growth group*. The difference dimension of G equals the dimension of the growth group and if the latter is zero, the size of the growth group equals the limit degree of G . In Section 4 we prove (i) (including the strong version) and (ii) of Theorem A. As an application of the strong version of (i) we prove the dimension theorem for affine difference algebraic groups. In Section 5 we introduce the limit degree of an affine difference algebraic group and relate our work to [KP07] by showing that the category of affine difference algebraic groups of limit degree one is equivalent to the category of affine algebraic σ -groups studied in [KP07]. Then in Section 6 we discuss a conjecture equivalent to Conjecture B and we prove (iii) of Theorem A. These questions are naturally related to the study of the connected components of an affine difference algebraic group. Finally, in the last section, we present the application of (i) of Theorem A to linear differential equations.

1 Preliminaries

In this section we recall some basic definitions from difference algebra and we define fundamental geometric concepts like difference varieties.

¹Some steps in this direction are already contained in the authors habilitation thesis ([Wib15]), which encompasses the first six sections of this article.

All rings are assumed to be commutative and unital. $\mathbb{N} = \{0, 1, 2, \dots\}$ and σ^0 is understood to be the identity map. By an “algebraic group” we mean an affine group scheme of finite type over a field. In particular, in positive characteristic, an algebraic group need not be reduced. A morphism $\mathcal{G} \rightarrow \mathcal{H}$ of algebraic groups is a *quotient map* if it is faithfully flat ([Mil17, Def. 5.5]). Equivalently, the dual map $k[\mathcal{H}] \rightarrow k[\mathcal{G}]$ is injective. Quotient maps are the appropriate scheme theoretic analog of surjective morphisms of smooth algebraic groups. (See [Mil17, Chapter 5] for more background.)

1.1 Difference algebra

Standard references for difference algebra are [Lev08] and [Coh65]. A *difference ring* (or σ -ring for short) is a ring R together with a ring endomorphism $\sigma: R \rightarrow R$. If σ is an automorphism, then R is called *inversive*. It is customary to use the same symbol σ for diverse endomorphisms. A *morphism of σ -rings* R and S is a morphism $\psi: R \rightarrow S$ of rings such that

$$\begin{array}{ccc} R & \xrightarrow{\psi} & S \\ \sigma \downarrow & & \downarrow \sigma \\ R & \xrightarrow{\psi} & S \end{array}$$

commutes. If R and S are σ -rings such that R is a subring of S and the inclusion map is a morphism of σ -rings, then R is a σ -subring of S . A *difference field* (or σ -field for short) is a difference ring whose underlying ring is a field.

Let k be a difference ring. A morphism of difference rings $k \rightarrow R$ is also called a k - σ -algebra. A *morphism of k - σ -algebras* is a morphism of k -algebras that is also a morphism of σ -rings. The category of k - σ -algebras is denoted by k - σ -Alg and $\text{Hom}(R, S)$ denotes the set of morphisms of k - σ -algebras from R to S .

For k - σ -algebras R and S the k -algebra $R \otimes_k S$ is naturally a σ -ring by $\sigma(r \otimes s) = \sigma(r) \otimes \sigma(s)$ for $r \in R$ and $s \in S$. Indeed, $R \otimes_k S$ is the coproduct of R and S in the category of k - σ -algebras.

A k - σ -subalgebra of a k - σ -algebra R is a k -subalgebra of R that is also σ -subring of R . For a subset $F \subseteq R$, the smallest k - σ -subalgebra of R that contains F is denoted by $k\{F\}$. It is called the k - σ -subalgebra of R σ -generated by F (over k). As a k -algebra, $k\{F\}$ is generated by all elements of the form $\sigma^i(f)$ with $i \in \mathbb{N}$ and $f \in F$. A k - σ -algebra R is called *finitely σ -generated* (over k) if there exists a finite subset $F \subseteq R$ such that $R = k\{F\}$.

The *ring of σ -polynomials over a σ -ring k in the σ -variables $y_1, \dots, y_n$* is the polynomial ring

$$k\{y\} = k\{y_1, \dots, y_n\} = k[y_1, \dots, y_n, \sigma(y_1), \dots, \sigma(y_n), \sigma^2(y_1), \dots, \sigma^2(y_n), \dots]$$

in the variables $y_1, \dots, y_n, \sigma(y_1), \dots, \sigma(y_n), \dots$ over k . It is naturally a k - σ -algebra with $\sigma: k\{y\} \rightarrow k\{y\}$ extended from $\sigma: k \rightarrow k$ as suggested by the naming of the variables. If R is a k - σ -algebra, $f \in k\{y\}$ a σ -polynomial and $x = (x_1, \dots, x_n) \in R^n$, the element $f(x) \in R$ is obtained by substituting $\sigma^i(x_j)$ for $\sigma^i(y_j)$. If $f(x) = 0$, then x is a *solution* of f .

An ideal $\mathfrak{a}$ of a σ -ring R is called a *difference ideal* (or σ -ideal for short) if $\sigma(\mathfrak{a}) \subseteq \mathfrak{a}$. In this case $R/\mathfrak{a}$ naturally inherits the structure of a σ -ring such that the canonical map $R \rightarrow R/\mathfrak{a}$ is a morphism of σ -rings. Let F be a subset of σ -ring R . The smallest σ -ideal of R containing F is denoted by $[F]$ and called the σ -ideal σ -generated by F . As an ideal $[F]$ is generated by all

elements of R that are of the form $\sigma^i(f)$ with $i \in \mathbb{N}$ and $f \in F$. A σ -ideal $\mathfrak{a}$ of a σ -ring R is *finitely σ -generated* if $\mathfrak{a} = [F]$ for a finite subset $F \subseteq \mathfrak{a}$.

1.2 Difference algebraic geometry

The various frameworks for algebraic geometry (e.g., Weil-style algebraic geometry, schemes, etc.) all have difference analogs. While the standard references [Lev08] and [Coh65] follow the style of Weil, in recent years, most authors follow a more utilitarian perspective and choose the geometric framework that is best suited for their problem at hand. It is well recognized that a functorial-schematic approach to algebraic groups has its benefits ([Gro70], [DG70], [Wat79], [Jan87], [Mil17]) and this is the strategy we will follow here. In other words, our approach to difference algebraic geometry is a natural adaptation of the approach of the above references from algebra to difference algebra, i.e., from algebraic equations to difference algebraic equations. Our approach is identical or equivalent to the approaches in [BW], [Kam13], [OW17], [MS11], [DVHW14] and [CK18]. However, it differs (in a more than formal way) from the approaches in [Hru04], [Lev08] and [CH99].

Throughout the article we work over a fixed σ -ring k . We are mainly interested in the case that k is a difference field.

Essentially, a *difference variety* (over k) is the set of solutions of a system of algebraic difference equations (over k). Let us make this more precise: Let R be a k - σ -algebra and $F \subseteq k\{y\} = k\{y_1, \dots, y_n\}$ a set of σ -polynomials over k . Then we may consider the R -rational solutions of F , that is

$$\mathbb{V}_R(F) = \{x \in R^n \mid f(x) = 0 \text{ for all } f \in F\}.$$

Note that $R \mapsto \mathbb{V}_R(F)$ is naturally a functor from k - σ -Alg to Sets, the category of sets. We denote this functor by $\mathbb{V}(F)$.

Definition 1.1. *Let k be a σ -ring. A difference variety (or σ -variety for short) over k is a functor from k - σ -Alg to Sets, that is of the form $\mathbb{V}(F)$, for some $n \geq 1$ and $F \subseteq k\{y_1, \dots, y_n\}$. A morphism of σ -varieties is a morphism of functors.*

It would be more accurate to add the word “affine” into Definition 1.1. However, to avoid endless iterations of the word “affine” we choose not to do so.

Let $F, G \subseteq k\{y\}$ and $X = \mathbb{V}(F)$, $Y = \mathbb{V}(G)$. If $F \subseteq G$, then $Y(R) \subseteq X(R)$ for every k - σ -algebra R and Y is a subfunctor of X . In this situation, Y is called a σ -closed σ -subvariety of X and write $Y \subseteq X$.

Let $X = \mathbb{V}(F)$ be a σ -variety, where $F \subseteq k\{y\} = k\{y_1, \dots, y_n\}$. Then

$$\mathbb{I}(X) = \{f \in k\{y\} \mid f(x) = 0 \text{ for all } k\text{-}\sigma\text{-algebras } R \text{ and all } x \in X(R)\} \quad (1)$$

is a σ -ideal of $k\{y\}$. The k - σ -algebra

$$k\{X\} = k\{y\}/\mathbb{I}(X)$$

is called the *coordinate ring* of X . As we may choose $R = k\{y\}/[F]$ in (1), we see that $\mathbb{I}(X) = [F] \subseteq k\{y\}$.

Let R be a k - σ -algebra and let $\bar{y} = (\bar{y}_1, \dots, \bar{y}_n) \in k\{X\}^n$ denote the images of $y_1, \dots, y_n$ in $k\{X\}$. The bijection

$$\text{Hom}(k\{X\}, R) \rightarrow X(R)$$

maps a morphism $\psi: k\{X\} \rightarrow R$ of k - σ -algebras to $\psi(\bar{y})$ is functorial in R . Thus the functor X is represented by $k\{X\}$. Conversely, since every finitely σ -generated k - σ -algebra can be written in the form $k\{y\}/[F]$, we see that a functor from k - σ -Alg to **Sets** that is representable by a finitely σ -generated k - σ -algebra is isomorphic (as a functor) to a σ -variety.

In the sequel we will allow ourselves the little abuse of notation to also call a functor isomorphic to a σ -variety a σ -variety. In particular, we will often identify X with the functor $\text{Hom}(k\{X\}, -)$. Thus a functor X from k - σ -Alg to **Sets** is a σ -variety if and only if it is representable by a finitely σ -generated k - σ -algebra $k\{X\}$. It is then clear from the Yoneda lemma that:

Remark 1.2. *The category of σ -varieties over k is anti-equivalent to the category of finitely σ -generated k - σ -algebras.*

If $\phi: X \rightarrow Y$ is a morphism of σ -varieties over k , the dual morphism of k - σ -algebras is denoted by $\phi^*: k\{Y\} \rightarrow k\{X\}$. As the tensor product is the coproduct in the category of k - σ -algebras it follows that:

Remark 1.3. *The category of σ -varieties has products. Indeed, if X and Y are σ -varieties over k , then $k\{X \times Y\} = k\{X\} \otimes_k k\{Y\}$. Moreover, there is a terminal object, namely, the functor represented by the k - σ -algebra k .*

In other words, the functor $R \mapsto (X \times Y)(R) = X(R) \times Y(R)$ is represented by $k\{X\} \otimes_k k\{Y\}$.

Let Y be a σ -variety and $f \in k\{Y\}$. Then, for any k - σ -algebra R , we have a well-defined map $f: Y(R) \rightarrow R$ given by evaluating a representative of f in $k\{y_1, \dots, y_n\}$ at an element of $Y(R) \subseteq R^n$. In a coordinate free manner $f: Y(R) \rightarrow R$ can be described as the map that sends $\psi \in Y(R) = \text{Hom}(k\{Y\}, R)$ to $\psi(f) \in R$.

Let X be a σ -closed σ -subvariety of Y . Then

$$\mathbb{I}(X) = \{f \in k\{Y\} \mid f(x) = 0 \text{ for all } k\text{-}\sigma\text{-algebras } R \text{ and all } x \in X(R)\} \quad (2)$$

is a σ -ideal of $k\{Y\}$. We call $\mathbb{I}(X) \subseteq k\{Y\}$ the *defining ideal of X* (in $k\{Y\}$). This notation is consistent with (II) in the sense that $\mathbb{I}(X)$ as defined in (II) is the defining ideal of X in $k\{y\} = k\{y_1, \dots, y_n\}$. Moreover, $\mathbb{I}(X) \subseteq k\{Y\}$ agrees with the image in $k\{Y\} = k\{y\}/\mathbb{I}(Y)$ of the defining ideal of X in $k\{y\}$. So $k\{X\} = k\{Y\}/\mathbb{I}(X)$.

Conversely, let $F \subseteq k\{Y\}$. Then we can define a σ -closed σ -subvariety $\mathbb{V}(F)$ of Y by

$$\mathbb{V}(F)(R) = \{x \in Y(R) \mid f(x) = 0 \text{ for all } f \in F\}$$

for any k - σ -algebra R .

Lemma 1.4. *Let Y be a σ -variety. Then $\mathbb{I}$ and $\mathbb{V}$ are mutually inverse bijections between the set of σ -closed σ -subvarieties of Y and the set of σ -ideals of $k\{Y\}$.*

Proof. Let $\mathfrak{a}$ be a σ -ideal of $k\{Y\}$. Clearly $\mathfrak{a} \subseteq \mathbb{I}(\mathbb{V}(\mathfrak{a}))$. Since we may choose $R = k\{Y\}/\mathfrak{a}$ in (2) it follows that $\mathfrak{a} = \mathbb{I}(\mathbb{V}(\mathfrak{a}))$.

Let X be σ -closed σ -subvariety of Y . Then $X = \mathbb{V}(\mathfrak{a})$ for some σ -ideal $\mathfrak{a}$ of $k\{Y\}$. So $\mathbb{V}(\mathbb{I}(X)) = \mathbb{V}(\mathbb{I}(\mathbb{V}(\mathfrak{a}))) = \mathbb{V}(\mathfrak{a}) = X$. $\square$

Note that if X is a σ -closed σ -subvariety of Y and R a k - σ -algebra, then $X(R) \subseteq Y(R)$ corresponds to $\{\psi \in \text{Hom}(k\{Y\}, R) \mid \mathbb{I}(X) \subseteq \ker(\psi)\} \subseteq \text{Hom}(k\{Y\}, R)$. If Y and Z are σ -closed σ -subvarieties of a σ -variety X , then we can define a subfunctor $Y \cap Z$ of X by $R \rightsquigarrow Y(R) \cap Z(R)$. Then $Y \cap Z$ is a σ -closed σ -subvariety of X , indeed, $\mathbb{I}(Y \cap Z) \subseteq k\{X\}$ is the ideal generated by $\mathbb{I}(Y)$ and $\mathbb{I}(Z)$.

The following lemma defines the difference analog of the scheme theoretic image ([Sta19, Tag 01R5]).

Lemma 1.5. *Let $\phi: X \rightarrow Y$ be a morphism of σ -varieties. There exists a unique σ -closed σ -subvariety $\phi(X)$ of Y with the following property. The morphism ϕ factors through $\phi(X)$ and if $Z \subseteq Y$ is a σ -closed σ -subvariety such that ϕ factors through Z then $\phi(X) \subseteq Z$.*

Proof. Let $\mathfrak{a}$ denote the kernel of $\phi^*: k\{Y\} \rightarrow k\{X\}$ and set $\phi(X) = \mathbb{V}(\mathfrak{a}) \subseteq Y$. As ϕ^* factors through $k\{Y\} \rightarrow k\{\phi(X)\} = k\{Y\}/\mathfrak{a}$, we see that ϕ factors through $\phi(X)$. If ϕ factors through Z , i.e., ϕ^* factors through $k\{Y\} \rightarrow k\{Z\} = k\{Y\}/\mathbb{I}(Z)$, then clearly $\mathbb{I}(Z) \subseteq \mathfrak{a}$. So $\phi(X) \subseteq Z$. $\square$

A morphism $\phi: X \rightarrow Y$ of σ -varieties is called a σ -closed embedding if ϕ induces an isomorphism between X and a σ -closed σ -subvariety of Y , i.e., $X \rightarrow \phi(X)$ is an isomorphism. We write $\phi: X \hookrightarrow Y$ to express that ϕ is a σ -closed embedding. In analogy to a well known result in algebraic geometry we have:

Lemma 1.6. *A morphism $\phi: X \rightarrow Y$ of σ -varieties is a σ -closed embedding if and only if $\phi^*: k\{Y\} \rightarrow k\{X\}$ is surjective.*

Proof. Let $\mathfrak{a}$ denote the kernel of $\phi^*: k\{Y\} \rightarrow k\{X\}$. The dual map to $X \rightarrow \phi(X)$ is $k\{Y\}/\mathfrak{a} \rightarrow k\{X\}$. It is an isomorphism if and only if ϕ^* is surjective. $\square$

Base change works as expected: Let k' be a k - σ -algebra and X a σ -variety over k . We can define a functor $X_{k'}$ from k' - σ -Alg to Sets by $X_{k'}(R') = X(R')$ for any k' - σ -algebra R' . Then $X_{k'}$ is a σ -variety over k' . Indeed, $k'\{X_{k'}\} = k\{X\} \otimes_k k'$. In terms of equations, this means that a system $F \subseteq k\{y\} = k\{y_1, \dots, y_n\}$ of algebraic difference equations over k is considered as a system $F \subseteq k'\{y\}$ of algebraic difference equations over k' . So if $k\{X\} = k\{y\}/[F]$ then $k'\{X_{k'}\} = k'\{y\}/[F]$.

1.3 Zariski closures

From now on we assume that our base σ -ring k is a σ -field.

Since algebraic equations can be interpreted as algebraic difference equations, it is clear that an affine scheme of finite type over k , can be interpreted as a σ -variety over k . In this subsection we make this more precise and we introduce some notation that will be useful in the coming sections. In particular, we define the Zariski closures of a σ -subvariety of a variety (cf. Section 4.3 in [Hru04] and Sections A.4 and A.5 in [DVHW14]).

For a k - σ -algebra R , let $R^\sharp$ denote the k -algebra obtained from R by forgetting the ring endomorphism $\sigma: R \rightarrow R$. Let $\mathcal{X}$ be an affine scheme of finite type over k . We can define a functor $[\sigma]_k \mathcal{X}$ from k - σ -Alg to Sets by

$$[\sigma]_k \mathcal{X}(R) = \mathcal{X}(R^\sharp)$$

for any k - σ -algebra R . We will show that $[\sigma]_k \mathcal{X}$ is a σ -variety over k . That is, we will construct $k\{[\sigma]_k \mathcal{X}\}$. Let A be a k -algebra. For every $i \geq 0$ let

$$\sigma^i A = A \otimes_k k$$

where the tensor product is formed by using $\sigma^i: k \rightarrow k$ on the right hand side. We consider $\sigma^i A$ as k -algebra via the right factor. We set

$$A[i] = A \otimes_k \sigma^0 A \otimes_k \cdots \otimes_k \sigma^i A.$$

We have inclusions $A[i] \hookrightarrow A[i+1]$ of k -algebras and the limit, i.e, the union $[\sigma]_k A$ of the $A[i]$'s is a k - σ -algebra, where for $(r_0 \otimes \lambda_0) \otimes \cdots \otimes (r_i \otimes \lambda_i) \in \sigma^0 A \otimes_k \cdots \otimes_k \sigma^i A = A[i]$ the map $\sigma: [\sigma]_k A \rightarrow [\sigma]_k A$ is given by

$$\sigma((r_0 \otimes \lambda_0) \otimes \cdots \otimes (r_i \otimes \lambda_i)) = (1 \otimes 1) \otimes (r_0 \otimes \sigma(\lambda_0)) \otimes \cdots \otimes (r_i \otimes \sigma(\lambda_i)) \in A[i+1].$$

The inclusion $A = A[0] \hookrightarrow [\sigma]_k A$ is characterized by the following universal property:

Lemma 1.7. *For every k -algebra A there exists a k - σ -algebra $[\sigma]_k A$ and a morphism $\psi: A \rightarrow [\sigma]_k A$ of k -algebras such that for every k - σ -algebra R and every morphism $\psi': A \rightarrow R$ of k -algebras there exists a unique morphism $\varphi: [\sigma]_k A \rightarrow R$ of k - σ -algebras making*

$$\begin{array}{ccc} A & \xrightarrow{\psi} & [\sigma]_k A \\ & \searrow \psi' & \swarrow \varphi \\ & R & \end{array}$$

commutative. □

In other words,

$$\text{Hom}([\sigma]_k A, R) \simeq \text{Hom}(A, R^\sharp) \tag{3}$$

and $[\sigma]_k$ is left adjoint to the forgetful functor $(-)^{\sharp}$.

Example 1.8. If $A = k[y_1, \dots, y_n]$, then $[\sigma]_k A = k\{y_1, \dots, y_n\}$. More generally, if $A = k[y_1, \dots, y_n]/(F)$, then $[\sigma]_k A = k\{y_1, \dots, y_n\}/[F]$.

Let $k[\mathcal{X}]$ denote the coordinate ring of $\mathcal{X}$, i.e., $\mathcal{X} = \text{Spec}(k[\mathcal{X}])$. Then (3) with $A = k[\mathcal{X}]$ shows that $[\sigma]_k \mathcal{X}$ is represented by $[\sigma]_k k[\mathcal{X}]$. If $F \subseteq k[\mathcal{X}]$ generates $k[\mathcal{X}]$ as a k -algebra, then $F \subseteq [\sigma]_k k[\mathcal{X}]$ generates $[\sigma]_k k[\mathcal{X}]$ as a k - σ -algebra. Therefore $[\sigma]_k \mathcal{X}$ is a σ -variety over k . Indeed, $k\{[\sigma]_k \mathcal{X}\} = [\sigma]_k k[\mathcal{X}]$. In the sequel, if confusion is unlikely, we will often write $\mathcal{X}$ instead of $[\sigma]_k \mathcal{X}$. In particular, we will write $k\{\mathcal{X}\}$ instead of $k\{[\sigma]_k \mathcal{X}\}$ and by a σ -closed σ -subvariety of $\mathcal{X}$, we mean a σ -closed σ -subvariety of $[\sigma]_k \mathcal{X}$.

To define the Zariski closures of a σ -closed σ -subvariety of $\mathcal{X}$ we will use notations for schemes similarly to the ones introduced for k -algebras above: For $i \geq 0$, we denote with $\sigma^i \mathcal{X}$ the scheme over k obtained from $\mathcal{X}$ by base change via $\sigma^i: k \rightarrow k$. Similarly, if $\phi: \mathcal{X} \rightarrow \mathcal{Y}$ is a morphism of schemes over k , then $\sigma^i \phi: \sigma^i \mathcal{X} \rightarrow \sigma^i \mathcal{Y}$ denotes the morphism of schemes over k obtained from ϕ by base change via $\sigma^i: k \rightarrow k$. We also set $\mathcal{X}[i] = \mathcal{X} \times^\sigma \mathcal{X} \times \cdots \times \sigma^i \mathcal{X}$.

Let Y be a σ -closed σ -subvariety of $\mathcal{X}$. Then Y is defined by a σ -ideal $\mathbb{I}(Y) \subseteq k\{\mathcal{X}\} = \bigcup_{i \geq 0} k[\mathcal{X}[i]]$. For $i \geq 0$, the closed subscheme $Y[i]$ of $\mathcal{X}[i]$ defined by $\mathbb{I}(Y) \cap k[\mathcal{X}[i]] \subseteq k[\mathcal{X}[i]]$ is called the *i-th order Zariski closure of Y in $\mathcal{X}$* .

For $i \geq 1$ we have morphisms of schemes over k

$$\pi_i: \mathcal{X}[i] \rightarrow \mathcal{X}[i-1], (x_0, \dots, x_i) \mapsto (x_0, \dots, x_{i-1})$$

and

$$\sigma_i: \mathcal{X}[i] \rightarrow \sigma(\mathcal{X}[i-1]) = \sigma \mathcal{X} \times \cdots \times \sigma^i \mathcal{X}, (x_0, \dots, x_i) \mapsto (x_1, \dots, x_i)$$

that form a commutative diagram:

$$\begin{array}{ccc} \mathcal{X}[i] & \xrightarrow{\pi_i} & \mathcal{X}[i-1] \\ \sigma_i \downarrow & & \downarrow \sigma_{i-1} \\ \sigma(\mathcal{X}[i-1]) & \xrightarrow{\sigma \pi_{i-1}} & \sigma(\mathcal{X}[i-2]) \end{array}$$

We have induced morphisms $\pi_i: Y[i] \rightarrow Y[i-1]$, and since $\mathbb{I}(Y) \subseteq k\{\mathcal{X}\}$ is a σ -ideal, we also have induced morphisms $\sigma_i: Y[i] \rightarrow \sigma(Y[i-1])$.

2 Difference algebraic groups: Examples and linearity

In this section we define σ -algebraic groups and present several examples. We also show that every σ -algebraic group is isomorphic to a σ -closed subgroup of some general linear group.

We work over a fixed σ -field k . Since the category of σ -varieties has products and a terminal object (Remark [L.3](#)) we can make the following definition.

Definition 2.1. *A σ -algebraic group over k is a group object in the category of σ -varieties over k .*

Alternatively, we could define a σ -algebraic group as a functor from $k\text{-}\sigma\text{-Alg}$ to **Groups**, the category of groups, that is representable by a finitely σ -generated k - σ -algebra. A *morphism of σ -algebraic groups* is a morphism of σ -varieties that respects the group structure. A *σ -closed embedding* $\phi: G \hookrightarrow H$ of σ -algebraic groups is a morphism of σ -algebraic groups that is a σ -closed embedding of σ -varieties.

Let G be a σ -algebraic group. A *σ -closed subgroup H of G* is a σ -closed σ -subvariety H of G such that $H(R)$ is a subgroup of $G(R)$ for any k - σ -algebra R . Then H itself is a σ -algebraic group. We write $H \leq G$ to express that H is a σ -closed subgroup of G .

The duality between affine group schemes and Hopf algebras carries over to the difference world in a straight forward manner.

Definition 2.2. A k - σ -Hopf algebra is a Hopf algebra A over k with the structure of a k - σ -algebra such that the Hopf-algebra structure maps $\Delta: A \rightarrow A \otimes_k A$, $S: A \rightarrow A$ and $\varepsilon: A \rightarrow k$ are morphisms of k - σ -algebras.

A k - σ -Hopf subalgebra of a k - σ -Hopf algebra is a k - σ -subalgebra that is Hopf subalgebra. A σ -Hopf ideal of a k - σ -Hopf algebra is a Hopf ideal that is also σ -ideal.

Remark 2.3. The category of σ -algebraic groups over k is anti-equivalent to the category of k - σ -Hopf algebras that are finitely σ -generated over k .

Proof. This follows from Remark 1.2 in an analogous fashion to Theorem 1.4 in [Wat79]. $\square$

In analogy to Section 2.1 in [Wat79], we obtain the following lemma from Lemma 1.4.

Lemma 2.4. Let G be a σ -algebraic group. There is a one-to-one correspondence between the σ -closed subgroups of G and the σ -Hopf ideals in $k\{G\}$. $\square$

Let us see some examples of σ -algebraic groups.

Example 2.5. Let V be a finite dimensional k -vector space. For every k - σ -algebra R let $\mathrm{GL}_V(R)$ denote the group of R -linear automorphisms of $V \otimes_k R$. Then GL_V is naturally a functor from k - σ -Alg to Groups. Indeed, GL_V is a σ -algebraic group: By choosing a basis $v_1, \dots, v_n$ of V , we can identify $\mathrm{GL}_V(R)$ with $\mathrm{GL}_n(R)$ and GL_V is represented by

$$k\{\mathrm{GL}_n\} = k\{x_{ij}, \frac{1}{\det(x)}\}.$$

More generally:

Example 2.6. Every algebraic group over k can be interpreted as a σ -algebraic group over k . Here, as throughout the text, by an algebraic group over k we mean an affine group scheme of finite type over k . Indeed, let $\mathcal{G}$ be an algebraic group over k and as in Section 1.3, let $R^\sharp$ denote the k -algebra obtained from the k - σ -algebra R by forgetting σ . Then

$$R \rightsquigarrow \mathcal{G}(R^\sharp)$$

is a functor from k - σ -Alg to Groups, i.e., $[\sigma]_k \mathcal{G}$ is a σ -algebraic group.

We will often write $\mathcal{G}$ instead of $[\sigma]_k \mathcal{G}$. In particular, by a σ -closed subgroup of $\mathcal{G}$ we mean a σ -closed subgroup of $[\sigma]_k \mathcal{G}$ and we write $k\{\mathcal{G}\}$ for $k\{[\sigma]_k \mathcal{G}\} = [\sigma]_k k[\mathcal{G}]$.

Example 2.7. Let $0 \leq \alpha_1 < \dots < \alpha_n$ and $1 \leq \beta_1, \dots, \beta_n$ be integers. We can define a σ -closed subgroup G of the multiplicative group $\mathbb{G}_m$ by

$$G(R) = \{g \in R^\times \mid \sigma^{\alpha_1}(g)^{\beta_1} \dots \sigma^{\alpha_n}(g)^{\beta_n} = 1\} \leq \mathbb{G}_m(R)$$

for any k - σ -algebra R . Similarly, we can define an endomorphism $\phi: \mathbb{G}_m \rightarrow \mathbb{G}_m$ of the multiplicative group (considered as a σ -algebraic group) by

$$\phi_R: \mathbb{G}_m(R) \rightarrow \mathbb{G}_m(R), \quad g \mapsto \sigma^{\alpha_1}(g)^{\beta_1} \dots \sigma^{\alpha_n}(g)^{\beta_n}$$

for any k - σ -algebra R .

Example 2.8. Every homogeneous linear difference equation

$$\sigma^n(y) + \lambda_{n-1}\sigma^{n-1}(y) + \cdots + \lambda_0 y = 0$$

over k defines a σ -closed subgroup G of the additive group $\mathbb{G}_a$, i.e.,

$$G(R) = \{g \in R \mid \sigma^n(g) + \lambda_{n-1}\sigma^{n-1}(g) + \cdots + \lambda_0 g = 0\} \leq \mathbb{G}_a(R)$$

for any k - σ -algebra R . We can define an endomorphism $\phi: \mathbb{G}_a \rightarrow \mathbb{G}_a$ of the additive group (considered as a σ -algebraic group) by

$$\phi_R: \mathbb{G}_a(R) \rightarrow \mathbb{G}_a(R), \quad g \mapsto \sigma^n(g) + \lambda_{n-1}\sigma^{n-1}(g) + \cdots + \lambda_0 g$$

for any k - σ -algebra R .

Example 2.9. The equations of the unitary group define a σ -closed subgroup of the general linear group:

$$G(R) = \{g \in \mathrm{GL}_n(R) \mid g\sigma(g)^T = \sigma(g)^T g = I_n\} \leq \mathrm{GL}_n(R)$$

for any k - σ -algebra R .

Example 2.10. For $m \geq 1$ we can define a σ -closed subgroup G of SL_n by

$$G(R) = \{g \in \mathrm{SL}_n(R) \mid \sigma^m(g) = g\} \leq \mathrm{SL}_n(R)$$

for any k - σ -algebra R .

Examples [2.9](#) and [2.10](#) can be generalized as follows:

Example 2.11. Let $m \geq 1$ be an integer, $\mathcal{G}$ an algebraic group over k and $\phi: \mathcal{G} \rightarrow \sigma^m \mathcal{G}$ a morphism of algebraic groups over k . There is a morphism $\sigma^m: \mathcal{G} \rightarrow \sigma^m \mathcal{G}$ of σ -algebraic groups over k , which, in terms of equations is given by applying σ^m to the coordinates. In terms of k - σ -algebras this morphism can be described as $\sigma^m(k\{\mathcal{G}\}) = k\{\mathcal{G}\} \otimes_k k \rightarrow k\{\mathcal{G}\}$, $f \otimes \lambda \mapsto \sigma^m(f)\lambda$. We can define a σ -closed subgroup G of $\mathcal{G}$ by

$$G(R) = \{g \in \mathcal{G}(R) \mid \sigma^m(g) = \phi(g)\} \leq \mathcal{G}(R)$$

for any k - σ -algebra R . Note that Example [2.9](#) ($\mathcal{G} = \mathrm{GL}_n$, $m = 1$, $\phi(g) = (g^{-1})^T$) and Example [2.10](#) ($\mathcal{G} = \mathrm{SL}_n$, $\phi(g) = g$) are special cases of this construction.

Example 2.12. For a k - σ -algebra R let $G(R) = R \times R^\times$. A straight forward computation shows that setting

$$(n_1, h_1) \cdot (n_2, h_2) = (n_1 + h_1\sigma(h_1)^{-1}n_2, h_1h_2)$$

for $(n_1, h_1), (n_2, h_2) \in G(R)$ defines a group structure on $G(R)$. Thus G is naturally a σ -algebraic group.

Example 2.13. Let k be a field of positive characteristic p and let q be a power of p . Consider k as a σ -field via the Frobenius, i.e., $\sigma(\lambda) = \lambda^q$ for $\lambda \in k$. An algebraic group $\mathcal{G}$ over k can be considered as a σ -algebraic group over k : We turn $k[\mathcal{G}]$ into a k - σ -algebra by setting $\sigma(f) = f^q$ for $f \in k[\mathcal{G}]$. Then clearly $k[\mathcal{G}]$ is a k - σ -Hopf algebra.

A finite group can be interpreted as an algebraic group, usually called a finite constant group. See e.g., [Mil17, 2.3] or [Wat79, Section 2.3]. The following example is a difference analog of this construction.

Example 2.14. Let G be a finite group and $\sigma: G \rightarrow G$ a group endomorphism. We define a functor G from $k\text{-}\sigma\text{-Alg}$ to **Groups** as follows: For a $k\text{-}\sigma$ -algebra R , let $G(R)$ denote the set of all locally constant maps $f: \text{Spec}(R) \rightarrow G$ such that

$$\begin{array}{ccc} \text{Spec}(R) & \xrightarrow{f} & G \\ \Sigma \downarrow & & \downarrow \sigma \\ \text{Spec}(R) & \xrightarrow{f} & G \end{array}$$

commutes, where $\Sigma(\mathfrak{p}) = \sigma^{-1}(\mathfrak{p})$ (for $\sigma: R \rightarrow R$). The group structure on $G(R)$ is given by pointwise multiplication. Note that the definition of $G(R)$ is functorial in R because a morphism $R_1 \rightarrow R_2$ of $k\text{-}\sigma$ -algebras induces a continuous map $\text{Spec}(R_2) \rightarrow \text{Spec}(R_1)$ such that

$$\begin{array}{ccc} \text{Spec}(R_2) & \longrightarrow & \text{Spec}(R_1) \\ \Sigma \downarrow & & \downarrow \Sigma \\ \text{Spec}(R_2) & \longrightarrow & \text{Spec}(R_1) \end{array}$$

commutes. To show that G is a σ -algebraic group, consider the k -algebra k^G of all maps from G to k (with pointwise addition and multiplication). For $g \in G$ let $\mathfrak{p}_g$ denote the prime ideal of k^G consisting of all functions that map g to 0. Note that every prime ideal of k^G is of the form $\mathfrak{p}_g$ for a unique $g \in G$.

For a k -algebra R , the map that associates to a morphism $\psi: k^G \rightarrow R$ of k -algebras, the map $\tilde{\psi}: \text{Spec}(R) \rightarrow G$, $\mathfrak{p} \mapsto g$, where g is the unique $g \in G$ such that $\psi^{-1}(\mathfrak{p}) = \mathfrak{p}_g$ is a bijection from the set of k -algebra morphisms $k^G \rightarrow R$ to the set of locally constant maps $\text{Spec}(R) \rightarrow G$ ([DG70, Chapter I, §1, 6.9]).

We define the structure of a $k\text{-}\sigma$ -algebra on k^G by $\sigma(h(g)) = \sigma(h(\sigma(g)))$ for $g \in G$ and $h: G \rightarrow k$. We claim that $\text{Hom}(k^G, R) \simeq G(R)$ for every $k\text{-}\sigma$ -algebra R . First, note that the bijection $G \rightarrow \text{Spec}(k^G)$, $g \mapsto \mathfrak{p}_g$ is such that

$$\begin{array}{ccc} G & \longrightarrow & \text{Spec}(k^G) \\ \sigma \downarrow & & \downarrow \Sigma \\ G & \longrightarrow & \text{Spec}(k^G) \end{array}$$

commutes. Since

$$\begin{array}{ccc} \text{Spec}(R) & \longrightarrow & \text{Spec}(k^G) \\ \Sigma \downarrow & & \downarrow \Sigma \\ \text{Spec}(R) & \longrightarrow & \text{Spec}(k^G) \end{array}$$

commutes for every $\psi \in \text{Hom}(k^G, R)$, we see that the map $\text{Hom}(k^G, R) \rightarrow G(R)$, $\psi \mapsto \tilde{\psi}$ is well-defined. It remains to show that a morphism $\psi: k^G \rightarrow R$ of k -algebras is a morphism of σ -rings if $\tilde{\psi}$ lies $G(R)$. In other words, we need to show that

$$\begin{array}{ccc} k^G & \xrightarrow{\psi} & R \\ \sigma \downarrow & & \downarrow \sigma \\ k^G & \xrightarrow{\psi} & R \end{array} \quad (4)$$

commutes, if the dual diagram

$$\begin{array}{ccc} \text{Spec}(k^G) & \longleftarrow & \text{Spec}(R) \\ \Sigma \uparrow & & \uparrow \Sigma \\ \text{Spec}(k^G) & \longleftarrow & \text{Spec}(R) \end{array}$$

commutes. As in Section 1.3, let ${}^\sigma R = R \otimes_k k$ denote the k -algebra obtained from the k -algebra R by base change via $\sigma: k \rightarrow k$. Then $\tilde{\sigma}: {}^\sigma R \rightarrow R$, $r \otimes \lambda \mapsto \sigma(r)\lambda$ is a morphism of k -algebras. We define $\tilde{\sigma}: {}^\sigma(k^G) \rightarrow k^G$ similarly. Then diagram (4) commutes if and only if the diagram

$$\begin{array}{ccc} {}^\sigma(k^G) & \xrightarrow{\sigma\psi} & {}^\sigma R \\ \tilde{\sigma} \downarrow & & \downarrow \tilde{\sigma} \\ k^G & \xrightarrow{\psi} & R \end{array} \quad (5)$$

of k -algebras commutes. Since two morphisms of k -algebras ${}^\sigma(k^G) \rightarrow R$ agree if they induce the same map $\text{Spec}(R) \rightarrow \text{Spec}({}^\sigma(k^G))$, it suffices to show that the diagram

$$\begin{array}{ccc} \text{Spec}({}^\sigma(k^G)) & \longleftarrow & \text{Spec}({}^\sigma R) \\ \uparrow & & \uparrow \\ \text{Spec}(k^G) & \longleftarrow & \text{Spec}(R) \end{array} \quad (6)$$

dual to (5) commutes. Let $i: R \rightarrow {}^\sigma R$, $r \mapsto r \otimes 1$, then $R \xrightarrow{i} {}^\sigma R \xrightarrow{\tilde{\sigma}} R$ equals σ and similarly for k^G in place of R . In the diagram

$$\begin{array}{ccccc} & & \text{Spec}(k^G) & \longleftarrow & \text{Spec}(R) \\ & \nearrow & \uparrow & & \uparrow \\ \Sigma & & \text{Spec}({}^\sigma(k^G)) & \longleftarrow & \text{Spec}({}^\sigma R) \\ & \nwarrow & \uparrow & & \uparrow \\ & & \text{Spec}(k^G) & \longleftarrow & \text{Spec}(R) \\ & & & & \nwarrow \\ & & & & \Sigma \end{array}$$

the upper square, the outer square and the left and right triangles commute. Moreover, the map $\text{Spec}({}^\sigma(k^G)) \rightarrow \text{Spec}(k^G)$ is bijective. It thus follows that diagram (6) commutes. So k^G represents G .

The Hopf algebra structure on k^G agrees with the one described in [Wat79, Section 2.3].

To show that any σ -algebraic group is isomorphic to a σ -closed subgroup of some general linear group, we need a lemma on Hopf algebras:

Lemma 2.15. *Let A be a k -Hopf algebra, B a k - σ -Hopf algebra and $A \rightarrow B$ a morphism of k -Hopf algebras. Then the morphism $[\sigma]_k A \rightarrow B$ of k - σ -algebras induced by Lemma 1.7 is a morphism of k -Hopf algebras.*

Proof. The comultiplication of $[\sigma]_k A$ is $[\sigma]_k(\Delta): [\sigma]_k A \rightarrow [\sigma]_k(A \otimes_k A) = [\sigma]_k A \otimes_k [\sigma]_k A$ where $\Delta: A \rightarrow A \otimes_k A$ is the comultiplication of A . All the subdiagrams with empty interior of

$$\begin{array}{ccc} [\sigma]_k A & \longrightarrow & [\sigma]_k(A \otimes_k A) \\ \uparrow & & \uparrow \\ A & \longrightarrow & A \otimes_k A \\ \downarrow & & \downarrow \\ B & \longrightarrow & B \otimes_k B \end{array}$$

commute. We have to show that the outer diagram commutes. But this follows from the uniqueness statement in Lemma 1.7. A similar argument applies for the counit. $\square$

Similar to (affine) algebraic groups, σ -algebraic groups can be linearized:

Proposition 2.16. *Let G be a σ -algebraic group over k . Then there exists a finite dimensional k -vector space V and a σ -closed embedding $G \hookrightarrow \mathrm{GL}_V$. In particular, G is isomorphic to a σ -closed subgroup of GL_n for some $n \geq 1$.*

Proof. Assume that $f_1, \dots, f_m \in k\{G\}$ generate $k\{G\}$ as a k - σ -algebra. By [Wat79, Section 3.3, p. 24] there exists a Hopf subalgebra A of $k\{G\}$ that contains $f_1, \dots, f_m$ and is finitely generated as a k -algebra. By [Wat79, Section 3.4, p. 25] there exists an integer $n \geq 1$ and a surjective morphism $k[\mathrm{GL}_n] \rightarrow A$ of Hopf algebras. By Lemma 1.7 the morphism $k[\mathrm{GL}_n] \rightarrow A \hookrightarrow k\{G\}$ of k -algebras extends to a morphism $k[\mathrm{GL}_n] \rightarrow k\{G\}$ of k - σ -algebras. Indeed, this is a morphism of k - σ -Hopf algebras (Lemma 2.15) and since $f_1, \dots, f_m$ lie in the image, it is surjective. Now the claim follows from Lemma 1.6. $\square$

3 Zariski closures of difference algebraic groups and the growth group

In this section we show that the eventual growth of the Zariski closures of a σ -closed subgroup G of an algebraic group $\mathcal{G}$ is governed by an algebraic group, called the *growth group* of G (with respect to the σ -closed embedding $G \hookrightarrow \mathcal{G}$). This result is key for obtaining the finiteness results in the next section. We also introduce the σ -dimension and the order of a σ -algebraic group.

Let k be a σ -field and $\mathcal{G}$ an algebraic group over k . Then, for ever $i \geq 0$, $\sigma^i \mathcal{G}$ and $\mathcal{G}[i] = \mathcal{G} \times {}^\sigma \mathcal{G} \times \dots \times {}^{\sigma^i} \mathcal{G}$ (see Section 1.3) are naturally algebraic groups over k . For every $i \geq 1$ the maps $\pi_i: \mathcal{G}[i] \rightarrow \mathcal{G}[i-1]$ and $\sigma_i: \mathcal{G}[i] \rightarrow {}^\sigma(\mathcal{G}[i-1])$ are morphisms of algebraic groups over k .

Let G be a σ -closed subgroup of $\mathcal{G}$. For every $i \geq 0$ we have an inclusion $k[\mathcal{G}[i]] \subseteq k\{\mathcal{G}\}$ of Hopf algebras. Since $\mathbb{I}(G) \subseteq k\{\mathcal{G}\}$ is a Hopf ideal, $\mathbb{I}(G) \cap k[\mathcal{G}[i]]$ is a Hopf ideal of $k[\mathcal{G}[i]]$. So the i -th order Zariski closure $G[i]$ of G in $\mathcal{G}$ is a closed subgroup of $\mathcal{G}[i]$. The maps $\pi_i: G[i] \rightarrow G[i-1]$ and $\sigma_i: G[i] \rightarrow {}^\sigma(G[i-1])$ are morphisms of algebraic groups over k and form a commutative diagram:

$$\begin{array}{ccc} G[i] & \xrightarrow{\pi_i} & G[i-1] \\ \sigma_i \downarrow & & \downarrow \sigma_{i-1} \\ {}^\sigma(G[i-1]) & \xrightarrow{{}^\sigma\pi_{i-1}} & {}^\sigma(G[i-2]) \end{array} \quad (7)$$

For $i \geq 1$ we set

$$\mathcal{G}_i = \ker(\pi_i) \leq G[i].$$

We also set $\mathcal{G}_0 = G[0]$. Because of (7) we have induced morphisms $\sigma_i: \mathcal{G}_i \rightarrow {}^\sigma(\mathcal{G}_{i-1})$ of algebraic groups over k .

Proposition 3.1. *For every $i \geq 1$ the map $\sigma_i: \mathcal{G}_i \rightarrow {}^\sigma(\mathcal{G}_{i-1})$ is a closed embedding and there exists an integer $m \geq 1$ such that $\sigma_i: \mathcal{G}_i \rightarrow {}^\sigma(\mathcal{G}_{i-1})$ is an isomorphism for every $i \geq m$.*

Proof. Let us start by describing σ_i in algebraic terms. Assume that $A = \{a_1, \dots, a_n\}$ generates $k[\mathcal{G}]$ as a k -algebra and let $\overline{A}$ denote the image of A in $k\{G\}$. So

$$k[\mathcal{G}] = k[A] \subseteq k[A, \sigma(A), \dots] = k\{G\}$$

and $k[G[i]] = k[\overline{A}, \dots, \sigma^i(\overline{A})]$. The morphism $\sigma_i: G[i] \rightarrow {}^\sigma(G[i-1])$ corresponds to the map

$$\sigma(k[\overline{A}, \dots, \sigma^{i-1}(\overline{A})]) \longrightarrow k[\overline{A}, \dots, \sigma^i(\overline{A})], \quad f \otimes \lambda \mapsto \sigma(f)\lambda$$

and the morphism $\sigma_i: \mathcal{G}_i \rightarrow {}^\sigma(\mathcal{G}_{i-1})$ corresponds to the map

$$\begin{aligned} \sigma(k[\overline{A}, \dots, \sigma^{i-1}(\overline{A})]) \otimes_{k[\overline{A}, \dots, \sigma^{i-2}(\overline{A})]} k &\longrightarrow k[\overline{A}, \dots, \sigma^i(\overline{A})] \otimes_{k[\overline{A}, \dots, \sigma^{i-1}(\overline{A})]} k \\ (f \otimes \lambda) \otimes \mu &\longmapsto \sigma(f) \otimes \sigma(\lambda)\mu \end{aligned}$$

where the tensor products are formed in virtue of the counit $\varepsilon: k\{G\} \rightarrow k$. Since $k[\overline{A}, \dots, \sigma^i(\overline{A})] \otimes_{k[\overline{A}, \dots, \sigma^{i-1}(\overline{A})]} k$ is generated as a k -algebra by the image of $\sigma^i(\overline{A})$, the above map is clearly surjective. Thus $\sigma_i: \mathcal{G}_i \rightarrow {}^\sigma(\mathcal{G}_{i-1})$ is a closed embedding.

To prove the second claim of the proposition, let us first assume that k is inversive. The map

$$\begin{aligned} \psi_i: k[\overline{A}, \dots, \sigma^{i-1}(\overline{A})] \otimes_{k[\overline{A}, \dots, \sigma^{i-2}(\overline{A})]} k &\longrightarrow k[\overline{A}, \dots, \sigma^i(\overline{A})] \otimes_{k[\overline{A}, \dots, \sigma^{i-1}(\overline{A})]} k \\ f \otimes \lambda &\longmapsto \sigma(f) \otimes \sigma(\lambda) \end{aligned}$$

is a morphism of rings but it is not a morphism of k -algebras. However, since k is inversive, it is surjective. We thus have a descending chain of closed subschemes

$$\mathcal{G}_0 \leftarrow \mathcal{G}_1 \leftarrow \mathcal{G}_2 \cdots$$

Since $\mathcal{G}_0$ is of finite type over k , this sequence must stabilize. That is, there exists an integer $m \geq 1$ such that ψ_i is bijective for every $i \geq m$. Since k is inversive,

$$k[\mathcal{G}_i] \rightarrow {}^\sigma(k[\mathcal{G}_i]), f \mapsto f \otimes 1$$

is bijective. It follows that for $i \geq m$, the morphism ${}^\sigma(k[\mathcal{G}_{i-1}]) \rightarrow k[\mathcal{G}_i]$ dual to σ_i is an isomorphism, since it can be obtained as the composition ${}^\sigma(k[\mathcal{G}_{i-1}]) \rightarrow k[\mathcal{G}_{i-1}] \xrightarrow{\psi_i} k[\mathcal{G}_i]$ of two bijective maps. This proves the proposition for k inversive.

The general case can be reduced to the inversive case: Let k^* denote the inversive closure of k ([Lev08, Definition 2.1.6]). So, in particular, k^* is an inversive σ -field extension of k . The formation of Zariski closures and of the $\mathcal{G}_i$ is compatible with base change. It therefore follows from the inversive case, that there exists an integer $m \geq 1$ such that for every $i \geq m$ the morphism $\sigma_i: \mathcal{G}_i \rightarrow {}^\sigma(\mathcal{G}_{i-1})$ becomes an isomorphism after base change from k to k^* . But then already σ_i must be an isomorphism for $i \geq m$. $\square$

Proposition 3.1 allows us to associate to the inclusion $G \leq \mathcal{G}$ an algebraic group, that measures the (eventual) growth of the Zariski closures $G[i]$ of G in $\mathcal{G}$.

Definition 3.2. Let $\mathcal{G}$ be an algebraic group and $G \leq \mathcal{G}$ a σ -closed subgroup. For $i \geq 1$ let $\mathcal{G}_i$ denote the kernel of the projection $\pi_i: G[i] \rightarrow G[i-1]$ between the Zariski closures of G in $\mathcal{G}$. Let $m \geq 0$ denote the smallest integer such that $\sigma_i: \mathcal{G}_i \rightarrow {}^\sigma(\mathcal{G}_{i-1})$ is an isomorphism for every $i > m$. Then $\mathcal{G}_m$ is called the growth group of G with respect to the σ -closed embedding $G \hookrightarrow \mathcal{G}$.

Example 3.3. Let $0 \leq \alpha_1 < \dots < \alpha_n$ and $1 \leq \beta_1, \dots, \beta_n$ be integers and $G \leq \mathbb{G}_m$ the σ -closed subgroup of the multiplicative group $\mathbb{G}_m$ given by

$$G(R) = \{g \in R^\times \mid \sigma^{\alpha_1}(g)^{\beta_1} \dots \sigma^{\alpha_n}(g)^{\beta_n} = 1\}$$

for every k - σ -algebra R . Then the growth group of G with respect to the given embedding $G \hookrightarrow \mathbb{G}_m$ is μ_{β_n} , where $\mu_{\beta_n}(T) = \{g \in T^\times \mid g^{\beta_n} = 1\}$ for any k -algebra T .

Example 3.4. Let G be a σ -closed subgroup of the additive group defined by a linear difference equation. (Cf. Example 2.3.) Then the growth group with respect to the given embedding $G \hookrightarrow \mathbb{G}_a$ is trivial.

Example 3.5. Let $\mathcal{G}$ be an algebraic group. The growth group with respect to the tautological embedding $G = [\sigma]_k \mathcal{G} \hookrightarrow \mathcal{G}$ is $\mathcal{G}$ itself.

The following example shows that the growth group does indeed depend on the embedding $G \hookrightarrow \mathcal{G}$ and therefore is not an invariant of G .

Example 3.6. Let $G = \mathbb{G}_m$ (considered as a σ -algebraic group). For $n \geq 1$ the σ -closed embedding

$$G \rightarrow \mathbb{G}_m^2, g \mapsto (g, \sigma(g)^n)$$

identifies G with the σ -closed subgroup $G \leq \mathbb{G}_m^2$ given by

$$G(R) = \{(g_1, g_2) \in \mathbb{G}_m(R)^2 \mid \sigma(g_1)^n = g_2\}$$

for any k - σ -algebra R . The growth group of G with respect to the embedding $G \hookrightarrow \mathbb{G}_m^2$ is $\mu_n \times \mathbb{G}_m$.

Even though the growth group itself does depend on the chosen embedding $G \hookrightarrow \mathcal{G}$, it carries some information that only depends on G . We will show below that the dimension of the growth group does not depend on the embedding $G \hookrightarrow \mathcal{G}$. In Section 5 we will see that also the size of the growth group is independent of the chosen embedding.

The following theorem can be seen as a group theoretic analog of the classical theorem on the existence of the so-called dimension polynomial of an extension of σ -fields ([Lev08, Theorem 4.2.1]). See also [Hru04, Lemma 4.21] (but note that we do not need any integrality assumptions).

Theorem 3.7. *Let $\mathcal{G}$ be an algebraic group and $G \leq \mathcal{G}$ a σ -closed subgroup. For $i \geq 0$ let $d_i = \dim(G[i])$ denote the dimension of the i -th order Zariski closure of G in $\mathcal{G}$. Then there exist integers $d, e \geq 0$ such that*

$$d_i = d(i + 1) + e \text{ for } i \gg 0.$$

The integer d only depends on G and not on the choice of $\mathcal{G}$ and the σ -closed embedding $G \hookrightarrow \mathcal{G}$. If $d = 0$, the integer e only depends on G and not on the choice of $\mathcal{G}$ and the σ -closed embedding $G \hookrightarrow \mathcal{G}$.

Proof. Let $\mathcal{G}_i$ denote the kernel of $G[i] \rightarrow G[i - 1]$. Then $\dim(G[i]) = \dim(G[i - 1]) + \dim(\mathcal{G}_i)$. Let $m \geq 0$ denote the smallest integer such that $\sigma_i: \mathcal{G}_i \rightarrow {}^\sigma(\mathcal{G}_{i-1})$ is an isomorphism for every $i > m$ (Proposition 3.1). It follows that for $i \gg 0$

$$\begin{aligned} \dim(G[i]) &= \dim(\mathcal{G}_i) + \cdots + \dim(\mathcal{G}_0) = \\ &= (i - m + 1) \dim(\mathcal{G}_m) + \dim(\mathcal{G}_{m-1}) + \cdots + \dim(\mathcal{G}_0) = \\ &= (i + 1) \dim(\mathcal{G}_m) + \dim(\mathcal{G}_{m-1}) + \cdots + \dim(\mathcal{G}_0) - m \dim(\mathcal{G}_m) = \\ &= d(i + 1) + e. \end{aligned}$$

By Proposition 3.1 we have $e \geq 0$.

Let us now show that $d = \dim(\mathcal{G}_m)$ is independent of the chosen embedding $G \hookrightarrow \mathcal{G}$. So let $G \hookrightarrow \mathcal{G}'$ be another σ -closed embedding. Let $G'[i]$ denote the i -th order Zariski closure of G in $\mathcal{G}'$ and let d'_i, d', e' have the analogous meaning. We have to show that $d = d'$.

Let A be a finite subset of $k\{G\}$ that generates $k[G[0]] \subseteq k\{G\}$ as a k -algebra. Similarly, let A' be a finite subset of $k\{G\}$ that generates $k[G[0]'] \subseteq k\{G\}$ as a k -algebra. Then $k[G[i]] = k[A, \dots, \sigma^i(A)]$ and there exists an integer $n \geq 0$ such that A' lies in $k[G[n]]$. Then

$$k[G[i]'] = k[A', \dots, \sigma^i(A')] \subseteq k[A, \dots, \sigma^{n+i}(A)] = k[G[n + i]].$$

Therefore $d'_i \leq d_{n+i}$ and for $i \gg 0$ we have $d'(i + 1) + e' \leq d(n + i + 1) + e$. Letting i tend to infinity we find $d' \leq d$. By symmetry, $d' = d$.

Let us now assume that $d = 0$. We have to show that e does not depend on the choice of the embedding $G \hookrightarrow \mathcal{G}$. To do this we will show that

$$e = \max \{ \dim(R) \mid R \text{ is a finitely generated } k\text{-subalgebra of } k\{G\} \}. \quad (8)$$

For $i \gg 0$ the finitely generated k -subalgebra $k[G[i]]$ of $k\{G\}$ has dimension e . Conversely, if R is a finitely generated k -subalgebra of $k\{G\}$, then R is contained in some $k[G[i]]$ and therefore $\dim(R) \leq e$. This proves (8). $\square$

Definition 3.8. Let G be a σ -algebraic group. The integer $d \geq 0$ defined in Theorem 3.7 above is called the σ -dimension of G and denoted by $\sigma\text{-dim}(G)$.

If $\sigma\text{-dim}(G) = 0$, the integer $e \geq 0$ defined in Theorem 3.7 is called the order of G and denoted by $\text{ord}(G)$. If G has positive σ -dimension the order of G is defined to be infinity.

The order is equivalent to the *total dimension* introduced in [Hru04] in a somewhat different setting. We have chosen to stick to the more traditional naming from [Lev08] and [Coh65].

Example 3.9. Let $n \in \mathbb{N}$ and let G be the σ -closed subgroup of $\mathbb{G}_a^2$ given by

$$G(R) = \{(g_1, g_2) \in R^2 \mid \sigma^n(g_1) = g_2\}$$

for any k - σ -algebra R . For $i \geq 0$ let $G[i]$ denote the i -th order Zariski closure of G in $\mathbb{G}_a$. As $k\{G\} = k[y_1, \dots, \sigma^{n-1}(y_1), y_2, \sigma(y_2), \dots]$ we see that $\dim(G[i]) = (i+1) + n$ for $i \gg 0$. In particular, G has σ -dimension one.

Example 3.10. Let $\mathcal{G}$ be an algebraic group. Then $\sigma\text{-dim}([\sigma]_k \mathcal{G}) = \dim(\mathcal{G})$. Indeed, if we tautologically consider $G = [\sigma]_k \mathcal{G}$ as a σ -closed subgroup of $\mathcal{G}$, then $G[i] = \mathcal{G} \times \dots \times \sigma^i \mathcal{G}$ and so $\dim(G[i]) = \dim(\mathcal{G})(i+1)$ for every $i \geq 0$. This also shows that either $\text{ord}(G) = \infty$ (if $\dim(\mathcal{G}) > 0$) or $\text{ord}(G) = 0$ (if $\dim(\mathcal{G}) = 0$).

The following example also motivates the naming “order”.

Example 3.11. Let $f = \sigma^n(y) + \lambda_{n-1}\sigma^{n-1}(y) + \dots + \lambda_0 y$ be a linear difference equation and G the σ -closed subgroup of $\mathbb{G}_a$ defined by f . Then $\text{ord}(G) = n$, i.e., the order of G equals the order of f .

Example 3.12. The σ -algebraic group from Example 3.3 has σ -dimension zero and order α_n .

Example 3.13. Let G be the σ -algebraic group from Example 2.11. Then $k\{G\} = k[\mathcal{G} \times \dots \times \sigma^{m-1} \mathcal{G}]$ and therefore $\sigma\text{-dim}(G) = 0$ and $\text{ord}(G) = m \dim(\mathcal{G})$.

Example 3.14. The σ -algebraic group from Example 2.13 has σ -dimension zero and order equal to the dimension of $\mathcal{G}$.

Example 3.15. The σ -algebraic group from Example 2.14 has σ -dimension zero and order zero.

From the proof of Theorem 3.7, we immediately obtain:

Corollary 3.16. Let G be a σ -algebraic group. Then the dimension of the growth group of G with respect to some σ -closed embedding $G \hookrightarrow \mathcal{G}$ of G into some algebraic group $\mathcal{G}$ equals the σ -dimension of G . In particular, the dimension of the growth group does not depend on the choice of the σ -closed embedding $G \hookrightarrow \mathcal{G}$. $\square$

We will show that our notions of dimension and order generalize the classical notions. (See page 394 in [Lev08].) Classically, the σ -dimension of a σ -variety X is defined by means of the σ -transcendence degree, which however only makes sense if $k\{X\}$ is an integral domain with $\sigma: k\{X\} \rightarrow k\{X\}$ injective. The σ -transcendence degree of a σ -field extension K/k is the largest integer $n \geq 1$ such that the σ -polynomial ring $k\{y_1, \dots, y_n\}$ may be embedded into K . (If no such integer exists the σ -transcendence degree is infinite.) See Section 4.1 in [Lev08] for more details on the σ -transcendence degree.

Proposition 3.17. *Let G be a σ -algebraic group such that $k\{G\}$ is a integral domain with $\sigma: k\{G\} \rightarrow k\{G\}$ injective. Then the σ -dimension of G equals the σ -transcendence degree of the field of fractions of $k\{G\}$ over k .*

If G is a σ -algebraic group such that $k\{G\}$ is an integral domain, then the order of G equals the transcendence degree of the field of fractions of $k\{G\}$ over k .

Proof. Let us fix a σ -closed embedding $G \hookrightarrow \mathcal{G}$. Assume that the finite set A generates $k[G[0]] \subseteq k\{G\}$ as a k -algebra. Let K denote the field of fractions of $k\{G\}$. Since $\sigma: k\{G\} \rightarrow k\{G\}$ is injective, K is naturally a σ -field extension of k and A generates K as a σ -field extension of k . Since $\text{trdeg}(k(A, \dots, \sigma^i(A))/k) = \dim(G[i])$, we see that $d(t+1) + e$ (with d and e as in Theorem 3.7) is the difference dimension polynomial (Definition 4.2.2 in [Lev08]) of the σ -field extension K/k associated with A . It follows from Theorem 4.2.1 (iii) in [Lev08] that $\sigma\text{-dim}(G) = d = \sigma\text{-trdeg}(K/k)$.

For the second claim, let again K denote the field of fractions of $k\{G\}$. If $\sigma\text{-dim}(G) > 0$, then it is clear from Theorem 3.7 that the transcendence degree of K over k is infinite. So $\text{ord}(G) = \text{trdeg}(K/k)$ in this case. If $\sigma\text{-dim}(G) = 0$, the claim follows from equation (8) above. $\square$

Example 3.18. Let G be the σ -algebraic group from Example 2.12. Then the coordinate ring of G is $k\{G\} = k\{y\} \otimes_k k\{x, x^{-1}\}$. The field of fractions of $k\{G\}$ is the field of fractions of a σ -polynomial ring in two σ -variables. Therefore the field of fractions of $k\{G\}$ has σ -transcendence degree two over k . (Cf. [Lev08, Prop. 4.1.6, p. 248].) Thus $\sigma\text{-dim}(G) = 2$ by Proposition 3.17.

4 Two finiteness theorems

There is no direct difference analog of Hilbert's basis theorem: There exist infinite strictly ascending chains of difference ideals in the σ -polynomial ring $k\{y_1, \dots, y_n\}$. (See [Coh65, Example 3, p. 73].) The Ritt-Raudenbush basis theorem in difference algebra ([RR39] or [Lev08, Theorem 2.5.11]) only asserts that every ascending chain of perfect difference ideals in $k\{y_1, \dots, y_n\}$ is finite. However, in our group theoretic setup the situation is better behaved: Let A be a finitely σ -generated k - σ -Hopf algebra. The first finiteness theorem (Theorem 4.1) asserts that every σ -Hopf ideal of A is finitely generated as a σ -ideal. The second finiteness theorem (Theorem 4.5) asserts that every k - σ -Hopf subalgebra of A is finitely σ -generated over k . In Section 6 we will prove a third finiteness theorem (Theorem 6.3): The set of minimal prime σ -ideals of A is finite.

Theorem 4.1. *Let H be a σ -algebraic group and $G \leq H$ a σ -closed subgroup. Then the defining ideal $\mathbb{I}(G) \subseteq k\{H\}$ of G is finitely generated as a σ -ideal.*

Proof. We may embed H as a σ -closed subgroup in some algebraic group $\mathcal{G}$. For example, we may choose $\mathcal{G} = \text{GL}_n$ by Proposition 2.16. If the defining ideal of G in $k\{\mathcal{G}\}$ is finitely σ -generated, then also the defining ideal of G in $k\{H\} = k\{\mathcal{G}\}/\mathbb{I}(H)$ is finitely σ -generated. We can therefore assume that $H = \mathcal{G}$.

As in Section 3, let $\mathcal{G}_i$ denote the kernel of the projection $\pi_i: G[i] \rightarrow G[i-1]$ between the Zariski closures of G in $\mathcal{G}$. By Proposition 3.1 there exists an integer $m \geq 1$ such that $\sigma_i: \mathcal{G}_i \rightarrow {}^\sigma\mathcal{G}_{i-1}$ is an isomorphism for every $i > m$. To prove the theorem we will show that

$\mathbb{I}(G[m]) = \mathbb{I}(G) \cap k[\mathcal{G}[m]]$ σ -generates $\mathbb{I}(G) \subseteq k\{\mathcal{G}\} = \cup_{i \geq 0} k[\mathcal{G}[i]]$. To do this it is sufficient to show that

$$\mathbb{I}(G[i]) = (\mathbb{I}(G[i-1]), \sigma(\mathbb{I}(G[i-1]))) \subseteq k[\mathcal{G}[i]] \quad (9)$$

for $i > m$. The ideal to the right-hand side of (9) defines an algebraic group

$$\mathcal{H}_i = (G[i-1] \times {}^{\sigma^i}\mathcal{G}) \cap (\mathcal{G} \times {}^{\sigma}(G[i-1])) \leq \mathcal{G}[i] = \mathcal{G} \times {}^{\sigma}\mathcal{G} \times \cdots \times {}^{\sigma^i}\mathcal{G}.$$

Clearly $G[i] \leq \mathcal{H}_i$ and the projection $\pi_i: \mathcal{H}_i \rightarrow G[i-1]$ is a quotient map, i.e., the dual map is injective.

The kernel of $\pi_i: \mathcal{H}_i \rightarrow G[i-1]$ is $1 \times {}^{\sigma}(\mathcal{G}_{i-1})$. Since $i > m$ we have $1 \times {}^{\sigma}(\mathcal{G}_{i-1}) = \mathcal{G}_i$. Thus the downwards arrows in the commutative diagram

$$\begin{array}{ccc} G[i] & \xrightarrow{\quad} & \mathcal{H}_i \\ & \searrow \pi_i & \swarrow \pi_i \\ & G[i-1] & \end{array}$$

are both quotient maps with the same kernel. This implies that $G[i] = \mathcal{H}_i$ and identity (9) is proved. $\square$

We have actually proved a slightly stronger statement which we record for later use.

Corollary 4.2. *Let $\mathcal{G}$ be an algebraic group and $G \leq \mathcal{G}$ a σ -closed subgroup. For $i \geq 0$ let $G[i]$ denote the i -th order Zariski closure of G in $\mathcal{G}$. Then there exists an integer $m \geq 0$ such that $\mathbb{I}(G[i]) = (\mathbb{I}(G[i-1]), \sigma(\mathbb{I}(G[i-1])))$ for $i > m$, i.e., $G[i] = (G[i-1] \times {}^{\sigma^i}\mathcal{G}) \cap (\mathcal{G} \times {}^{\sigma}(G[i-1]))$. $\square$*

Corollary 4.3. *Every descending chain of σ -closed subgroups of a σ -algebraic group is finite.*

Proof. A descending chain $H_1 \geq H_2 \geq \cdots$ of σ -closed subgroups of a σ -algebraic group G corresponds to an ascending chain $\mathbb{I}(H_1) \subseteq \mathbb{I}(H_2) \subseteq \cdots$ of σ -Hopf ideals in $k\{G\}$. By Theorem 4.1 the union $\bigcup \mathbb{I}(H_i)$ (which corresponds to the intersection $\bigcap H_i$) is finitely generated as a σ -ideal. Thus there exists an integer $n \geq 1$ such that $\bigcup \mathbb{I}(H_i) = \mathbb{I}(H_n)$. Then $H_{i+1} = H_i$ for $i \geq n$. $\square$

To prove the second finiteness theorem we need a lemma on k - σ -Hopf algebras.

Lemma 4.4. *Let A be a k - σ -Hopf algebra. Then every finite subset of A is contained in a finitely σ -generated k - σ -Hopf subalgebra.*

Proof. By [Wat79, Section 3.3] a finite subset of A is contained in a Hopf subalgebra B that is finitely generated as a k -algebra. Then $k\{B\} \subseteq A$ is finitely σ -generated over k and since the comultiplication and the antipode are σ -morphisms, $k\{B\}$ is a Hopf subalgebra. $\square$

Theorem 4.5. *Let A be a k - σ -Hopf algebra that is finitely σ -generated over k and $B \subseteq A$ a k - σ -Hopf subalgebra. Then B is finitely σ -generated over k .*

Proof. For a Hopf subalgebra C of A let $\mathfrak{m}_C \subseteq C$ denote the kernel of the counit $\varepsilon: C \rightarrow k$. The ideal $(\mathfrak{m}_B) \subseteq A$ is a σ -Hopf ideal. By Theorem 4.1 it is finitely σ -generated. So there exists a finite set $F \subseteq \mathfrak{m}_B$ such that $[F] = (\mathfrak{m}_B)$. By Lemma 4.4 there exists a finitely σ -generated k - σ -Hopf subalgebra C of B containing F . Then $(\mathfrak{m}_C) = (\mathfrak{m}_B)$. By Corollary 3.10 in [Tak72] the mapping $C \mapsto (\mathfrak{m}_C)$ from Hopf subalgebras to Hopf ideals is injective. Thus $B = C$ is finitely σ -generated over k . $\square$

As an application of Corollary 4.2, we will prove a dimension theorem for σ -algebraic groups. A dimension theorem for differential algebraic groups has been proved in [Sit74]. It is interesting to note that the dimension theorem fails for difference varieties. See [Coh65, Chapter 8, Section 8].

Theorem 4.6. *Let H_1 and H_2 be σ -closed subgroups of a σ -algebraic group G . Then*

$$\sigma\text{-dim}(H_1 \cap H_2) + \sigma\text{-dim}(G) \geq \sigma\text{-dim}(H_1) + \sigma\text{-dim}(H_2) \quad (10)$$

and

$$\text{ord}(H_1 \cap H_2) + \text{ord}(G) \geq \text{ord}(H_1) + \text{ord}(H_2). \quad (11)$$

Proof. Let $\mathcal{G}$ be an algebraic group containing G as a σ -closed subgroup. We consider the Zariski closures inside $\mathcal{G}$. By Corollary 4.2 there exists an integer $m \geq 0$ such that

$$\mathbb{I}((H_1 \cap H_2)[i]) = (\mathbb{I}((H_1 \cap H_2)[i-1]), \sigma(\mathbb{I}((H_1 \cap H_2)[i-1])))$$

for $i > m$. Since $\mathbb{I}(H_1 \cap H_2) = \mathbb{I}(H_1) + \mathbb{I}(H_2)$ there exists $n \geq m$ such that

$$\mathbb{I}((H_1 \cap H_2)[m]) \subseteq \mathbb{I}(H_1[n]) + \mathbb{I}(H_2[n]) = \mathbb{I}(H_1[n] \cap H_2[n]).$$

But then

$$\mathbb{I}((H_1 \cap H_2)[m+i]) \subseteq \mathbb{I}(H_1[n+i] \cap H_2[n+i]) \quad (12)$$

for every $i \geq 0$ and so

$$H_1[n+i] \cap H_2[n+i] \leq (H_1 \cap H_2)[m+i] \times \sigma^{m+i+1}\mathcal{G} \times \cdots \times \sigma^{n+i}\mathcal{G}.$$

Therefore

$$\dim(H_1[n+i] \cap H_2[n+i]) \leq \dim((H_1 \cap H_2)[m+i]) + (n-m)\dim(\mathcal{G})$$

and so

$$\begin{aligned} \dim((H_1 \cap H_2)[m+i]) &\geq \dim(H_1[n+i] \cap H_2[n+i]) - (n-m)\dim(\mathcal{G}) \\ &\geq \dim(H_1[n+i]) + \dim(H_2[n+i]) - \dim(G[n+i]) - (n-m)\dim(\mathcal{G}). \end{aligned}$$

Now using Theorem 3.7 and comparing the coefficients of i yields identity (10).

It remains to prove (11). Obviously this is true if $\text{ord}(G) = \infty$. So we can assume $\text{ord}(G) < \infty$, i.e., $\sigma\text{-dim}(G) = 0$. Note that (12) implies that the intersection of $\mathbb{I}(H_1[n+i] \cap H_2[n+i])$ with $k[\mathcal{G}[m+i]]$ equals $\mathbb{I}((H_1 \cap H_2)[m+i])$. This means that the morphism of algebraic groups

$$\phi: H_1[n+i] \cap H_2[n+i] \rightarrow (H_1 \cap H_2)[m+i]$$

induced from the projection $\mathcal{G} \times {}^\sigma\mathcal{G} \times \cdots \times {}^{\sigma^{n+i}}\mathcal{G} \rightarrow \mathcal{G} \times {}^\sigma\mathcal{G} \times \cdots \times {}^{\sigma^{m+i}}\mathcal{G}$ is a quotient map. Since $\sigma\text{-dim}(H_1) = 0$, the kernel of the projections $H_1[n+i] \rightarrow H_1[m+i]$ is finite for $i \gg 0$. Therefore, also ϕ has finite kernel and it follows that for $i \gg 0$

$$\begin{aligned} \text{ord}(H_1 \cap H_2) &= \dim((H_1 \cap H_2)[m+i]) = \dim(H_1[n+i] \cap H_2[n+i]) \\ &\geq \dim(H_1[n+i]) + \dim(H_2[n+i]) - \dim(G[n+i]) \\ &= \text{ord}(H_1) + \text{ord}(H_2) - \text{ord}(G). \end{aligned}$$

□

5 The limit degree

The limit degree is a classical and important numerical invariant of extensions of difference fields. See [Lev08, Section 4.3]. Based on the results of Section 3, we introduce the limit degree of a difference algebraic group. A connection between the two notions is that the limit degree of a σ -Picard-Vessiot extension (in the sense of [DVHW14]) agrees with the limit degree of the corresponding σ -Galois group. We also note that, in our restricted affine setting, difference algebraic groups of limit degree one correspond to *algebraic σ -groups* ([KP07]).

By the *size* $|\mathcal{G}|$ of an algebraic group $\mathcal{G}$ we mean the dimension of $k[\mathcal{G}]$ as a k -vector space. So the size is either a non-negative integer or ∞ (and may exceed $|\mathcal{G}(k)|$). In the sequel we will employ the usual rules for calculating with the symbol ∞ . E.g., if $\mathcal{G}_1 \xrightarrow{\phi_1} \mathcal{G}_2 \xrightarrow{\phi_2} \mathcal{G}_3$ are quotient maps of algebraic groups, then

$$|\ker(\phi_2 \circ \phi_1)| = |\ker(\phi_2)| \cdot |\ker(\phi_1)|. \quad (13)$$

In Section 3 we have seen that the dimension of the growth group of a σ -closed subgroup G of an algebraic group $\mathcal{G}$ only depends on G . The following proposition shows that the same is true for the size of the growth group.

Proposition 5.1. *Let G be a σ -algebraic group and $G \hookrightarrow \mathcal{G}$ a σ -closed embedding. Then the size of the growth group of G with respect to the embedding $G \hookrightarrow \mathcal{G}$ does not depend on the choice of $\mathcal{G}$ and the σ -closed embedding.*

Proof. For $i \geq 0$ let $G[i]$ denote the i -th order Zariski closure of G in $\mathcal{G}$ and $\mathcal{G}_i$ the kernel of the projection $\pi_i: G[i] \rightarrow G[i-1]$. By Proposition 3.1 the integer $d = |\mathcal{G}_i|$ does not depend on i for $i \gg 0$. Assume that the finite set A generates $k[G[0]] \subseteq k\{G\}$ as a k -algebra. Then A also σ -generates $k\{G\}$ as a k - σ -algebra.

Let $\mathcal{G}'$ be another algebraic group and $G \hookrightarrow \mathcal{G}'$ a σ -closed embedding. Let $G[i]'$ denote the i -th order Zariski closure of G in $\mathcal{G}'$ and let d' and A' be as above. We have to show that $d = d'$.

Since A , as well as A' , σ -generate $k\{G\}$, there exists an integer $m \geq 1$ such that $A' \in k[A, \dots, \sigma^m(A)]$ and $A \in k[A', \dots, \sigma^m(A')]$. Then, for $i \geq 0$, we have $k[A', \dots, \sigma^i(A')] \subseteq k[A, \dots, \sigma^{m+i}(A)]$ and $k[A, \dots, \sigma^i(A)] \subseteq k[A', \dots, \sigma^{m+i}(A')]$. So for $j \geq m$:

$$k[A, \dots, \sigma^i(A)] \subseteq k[A', \dots, \sigma^{m+i}(A')] \subseteq k[A', \dots, \sigma^{j+i}(A')] \subseteq k[A, \dots, \sigma^{m+j+i}(A)].$$

These inclusions of Hopf algebras correspond to quotient maps of algebraic groups

$$G[m+j+i] \rightarrow G[j+i]' \rightarrow G[m+i]' \rightarrow G[i].$$

We have $|\ker(G[m+j+i] \rightarrow G[i])| \geq |\ker(G[j+i]' \rightarrow G[m+i]')|$ by (13). But by (13) and Proposition 3.1 we also have

$$|\ker(G[m+j+i] \rightarrow G[i])| = d^{m+j} \quad \text{and} \quad |\ker(G[j+i]' \rightarrow G[m+i]')| = d'^{j-m}$$

for $i \gg 0$. Consequently, $d^{m+j} \geq d'^{j-m}$. Letting j tend to infinity, we find $d \geq d'$. By symmetry, $d = d'$. $\square$

Definition 5.2. Let G be a σ -algebraic group. Choose an algebraic group $\mathcal{G}$ and a σ -closed embedding $G \hookrightarrow \mathcal{G}$. The size of the growth group of G with respect to the σ -closed embedding $G \hookrightarrow \mathcal{G}$ is called the *limit degree* of G and is denoted by $\text{ld}(G)$. By Proposition 5.1 the limit degree of G does not depend on the choice of $\mathcal{G}$ and the σ -closed embedding $G \hookrightarrow \mathcal{G}$.

The expression “limit degree” is motivated by the fact that $\text{ld}(G) = \lim_{i \rightarrow \infty} \deg(\pi_i)$, where $\deg(\pi_i)$ denotes the degree of the projection $\pi_i: G[i] \rightarrow G[i-1]$. The naming is also motivated by Lemma 5.6 below. We note that, by Corollary 3.16, the limit degree of a σ -algebraic group is finite if and only if it has σ -dimension zero.

Example 5.3. Let $0 \leq \alpha_1 < \dots < \alpha_n$ and $1 \leq \beta_1, \dots, \beta_n$ be integers and $G \leq \mathbb{G}_m$ the σ -closed subgroup of the multiplicative group $\mathbb{G}_m$ given by

$$G(R) = \{g \in R^\times \mid \sigma^{\alpha_1}(g)^{\beta_1} \dots \sigma^{\alpha_n}(g)^{\beta_n} = 1\}$$

for every k - σ -algebra R . Then $\text{ld}(G) = \beta_n$ by Example 3.3.

Example 5.4. By Example 3.4 the limit degree of a σ -closed subgroup of $\mathbb{G}_a$ defined by a linear difference equation is one.

Example 5.5. Let $\mathcal{G}$ be an algebraic group. Then $\text{ld}([\sigma]_k \mathcal{G}) = |\mathcal{G}|$ by Example 3.5.

We will next show that our definition of the limit degree corresponds to the classical notion (whenever both notions make sense). To this end, let us recall the definition of the limit degree of an extension K/k of σ -fields. Assume that there exists a finite set $A \subseteq K$ such that $a, \sigma(A), \dots$ generates K as a field extension of k , then the limit degree $\text{ld}(K/k)$ is the limit $\lim_{i \rightarrow \infty} d_i$, where d_i is the degree of the field extension $k(A, \dots, \sigma^i(A))/k(A, \dots, \sigma^{i-1}(A))$. The limit exists and does not depend on the choice of A ([Lev08, Section 4.3]).

Lemma 5.6. Let G be a σ -algebraic group such that $k\{G\}$ is an integral domain and $\sigma: k\{G\} \rightarrow k\{G\}$ is injective. Then the limit degree of G equals the limit degree of the field of fractions of $k\{G\}$ over k .

Proof. Let $\mathcal{G}$ be an algebraic group containing G as a σ -closed subgroup. For $i \geq 0$ let $G[i]$ denote the i -th order Zariski closure of G in $\mathcal{G}$ and let $A \subseteq k[G[0]]$ be a finite set that generates $k[G[0]] \subseteq k\{G\}$ as a k -algebra. Let K denote the field of fractions of $k\{G\}$. Then $A, \sigma(A), \dots$ generates K as a field extension of k and $k(A, \sigma(A), \dots, \sigma^i(A))$ is the field of fractions of $k[G[i]]$. Therefore the degree of the field extension

$$k(A, \dots, \sigma^i(A))/k(A, \dots, \sigma^{i-1}(A))$$

equals the degree of the projection $G[i] \rightarrow G[i-1]$. $\square$

It is well-known that a finitely σ -generated extension of σ -fields has limit degree one if and only if the extension is finitely generated as a field extension ([Lev08, Prop. 4.3.12]). A similar statement is true for difference Hopf algebras:

Lemma 5.7. *Let G be a σ -algebraic group. Then $\text{ld}(G) = 1$ if and only if $k\{G\}$ is finitely generated as a k -algebra.*

Proof. Fix a σ -closed embedding $G \hookrightarrow \mathcal{G}$ and let $G[i]$ denote the i -th order Zariski closure of G in $\mathcal{G}$. So $k\{G\} = \cup_{i \geq 0} k[G[i]]$. If $\text{ld}(G) = 1$, there exists an integer $m \geq 0$ such that the quotient maps $\pi_i: G[i] \rightarrow G[i-1]$ have trivial kernel for $i > m$. So π_i is an isomorphism and therefore $k[G[i]] = k[G[i-1]]$. Consequently, $k\{G\} = k[G[m]]$ is finitely generated as a k -algebra.

Conversely, if $k\{G\}$ is a finitely generated k -algebra, we can consider the algebraic group $\mathcal{G}$ associated with the Hopf algebra $k\{G\}$, i.e., $k[\mathcal{G}] = k\{G\}$ as k -algebras. By Lemma 2.15 the morphism $k[\mathcal{G}] \rightarrow k\{G\}$ induced from the identity map $k[\mathcal{G}] \rightarrow k[\mathcal{G}]$ is a morphism of k - σ -Hopf algebras. With respect to the corresponding σ -closed embedding $G \hookrightarrow \mathcal{G}$ we have $k\{G\} = k[G[0]] = k[G[1]] = \dots$ and therefore the associated growth group is trivial. Thus $\text{ld}(G) = 1$. $\square$

Example 5.8. It is clear from Lemma 5.7 that the σ -algebraic groups in Examples 2.11, 2.13 and 2.14 have limit degree one.

We conclude this section by explaining the connection between the category of algebraic σ -groups introduced in [KP07] and affine difference algebraic groups of limit degree one. Let us begin by recalling the definition of algebraic σ -groups from [KP07]. Let k be a σ -field. An *algebraic σ -variety*² over k is a scheme $\mathcal{X}$ of finite type over k together with a morphism $\tilde{\sigma}: \mathcal{X} \rightarrow {}^\sigma\mathcal{X}$ of schemes over k . Here, as in Section 1.3, ${}^\sigma\mathcal{X}$ denotes the scheme over k obtained from $\mathcal{X}$ by base change via $\sigma: k \rightarrow k$. A morphism between algebraic σ -varieties is a morphism $\phi: \mathcal{X} \rightarrow \mathcal{Y}$ of schemes over k such that

$$\begin{array}{ccc} \mathcal{X} & \xrightarrow{\tilde{\sigma}} & {}^\sigma\mathcal{X} \\ \phi \downarrow & & \downarrow {}^{\sigma\phi} \\ \mathcal{Y} & \xrightarrow{\tilde{\sigma}} & {}^\sigma\mathcal{Y} \end{array}$$

commutes. An *algebraic σ -group* is a group object in the category of algebraic σ -varieties. Equivalently, an algebraic σ -group is a (not necessarily affine) algebraic group $\mathcal{G}$ over k together with a morphism $\tilde{\sigma}: \mathcal{G} \rightarrow {}^\sigma\mathcal{G}$ of algebraic groups. The category of *affine algebraic σ -groups* consists of the algebraic σ -groups whose underlying scheme is affine; the morphisms are morphism of algebraic σ -varieties that are also morphisms of algebraic groups.

Proposition 5.9. *The category of affine algebraic σ -groups is equivalent to the category of σ -algebraic groups of limit degree one.*

²The assumptions in [KP07] on k and $\mathcal{X}$ are slightly more restrictive but this is irrelevant for our discussion here.

Proof. Let R be a k -algebra. To define a k - σ -algebra structure on R is equivalent to defining a morphism of k -algebras $\bar{\sigma}: {}^\sigma R \rightarrow R$: Given $\sigma: R \rightarrow R$, we can define

$$\bar{\sigma}: {}^\sigma R \rightarrow R, \quad r \otimes \lambda \mapsto \sigma(r)\lambda.$$

Conversely, given $\bar{\sigma}: {}^\sigma R \rightarrow R$, we can define $\sigma: R \xrightarrow{\text{id} \otimes 1} R \otimes_k k = {}^\sigma R \xrightarrow{\bar{\sigma}} R$. Moreover, if R and S are k - σ -algebras and $\psi: R \rightarrow S$ is a morphism of k -algebras, then ψ is a morphism of k - σ -algebras if and only if

$$\begin{array}{ccc} {}^\sigma R & \xrightarrow{\bar{\sigma}} & R \\ \sigma\psi \downarrow & & \downarrow \psi \\ {}^\sigma S & \xrightarrow{\bar{\sigma}} & S \end{array}$$

commutes.

Dualizing the definition, an affine algebraic σ -group $\mathcal{G}$ corresponds to a finitely generated Hopf algebra $k[\mathcal{G}]$ together with a morphism of Hopf algebras $\bar{\sigma} = (\tilde{\sigma})^*: {}^\sigma(k[\mathcal{G}]) \rightarrow k[\mathcal{G}]$. By the remark from the beginning of the proof, the statement that $\bar{\sigma}$ is a morphism of Hopf algebras corresponds to the statement that $k[\mathcal{G}]$ is a k - σ -Hopf algebra. Thus the category of affine algebraic σ -groups is anti-equivalent to the category of k - σ -Hopf algebras that are finitely generated as k -algebras. Now the claim follows from Remark 2.3 and Lemma 5.7. $\square$

6 Connected components of difference algebraic groups

In this section we study the connected components of $\text{Spec}(k\{G\})$ for a difference algebraic group G . Our main result is that there are only finitely many invariant connected components. This result can be reinterpreted as a positive answer (in a special case) to a question raised by E. Hrushovski.

6.1 Two equivalent conjectures

In [Hru04, Section 4.6] E. Hrushovski raised the question whether or not it is possible to strengthen the classical Ritt-Raudenbusch basis theorem ([Lev08, Theorem 2.5.11]). For clarity, let us state the question as a conjecture:

Conjecture 6.1. *Let k be a σ -field and R a finitely σ -generated k - σ -algebra. Then every ascending chain of radical, well-mixed σ -ideals in R is finite.*

Recall that a σ -ideal $\mathfrak{a}$ is *well-mixed*, if $ab \in \mathfrak{a}$ implies $a\sigma(b) \in \mathfrak{a}$. E. Hrushovski proved Conjecture 6.1 under certain additional assumptions on R ([Hru04, Lemma 4.35]). Moreover, J. Wang ([Wan18] [Wan17]) proved the conjecture (appropriately reformulated) for monomial and binomial difference ideals. In [Lev15] A. Levin showed that the conjecture fails if the assumption that the σ -ideals are radical is dropped.

A prime σ -ideal $\mathfrak{p}$ of a σ -ring R is a σ -ideal that is a prime ideal. It is a *minimal prime σ -ideal* if for every prime σ -ideal $\mathfrak{q}$ of R with $\mathfrak{q} \subseteq \mathfrak{p}$ we have $\mathfrak{q} = \mathfrak{p}$. We will show below that Conjecture 6.1 is equivalent to the following conjecture.

Conjecture 6.2. *Let k be a σ -field and R a finitely σ -generated k - σ -algebra. Then the set of minimal prime σ -ideals of R is finite.*

The main result of this section is a special case of Conjecture [6.2](#).

Theorem 6.3. *Conjecture [6.2](#) holds under the additional assumption that R can be equipped with the structure of a k - σ -Hopf algebra.*

The proof of Theorem [6.3](#) is given at the end of this section. We will first show that the two conjectures are equivalent. To this end we need a basic topological lemma. Recall that a topological space X is *Noetherian* if every descending chain of closed subsets of X is finite.

Lemma 6.4. *A topological space is Noetherian if and only if*

- (i) *every descending chain of irreducible closed subsets is finite and*
- (ii) *every closed subset is a finite union of irreducible closed subsets.*

Assume that X is a Noetherian topological space. Then clearly (i) is satisfied and it is also well-known that (ii) holds for X ([Sta19](#), [Lemma 5.9.2, Tag 0050](#)).

The proof of the reverse direction is a variation of the proof of König's Lemma: Assume that X is a topological space satisfying (i) and (ii). Let

$$X_1 \supseteq X_2 \supseteq \dots \quad (14)$$

be a descending chain of closed subsets of X . Using (ii), for every $i \geq 1$, we may write $X_i = Y_{i,1} \cup \dots \cup Y_{i,n_i}$ as an irredundant union of irreducible closed subsets $Y_{i,j}$ of X . We define a directed graph as follows: The set of vertices is $\{(i, j) \mid 1 \leq i \text{ and } 1 \leq j \leq n_i\}$ and there is an arrow from (i, j) to (i', j') if $i' = i - 1$ and $Y_{i,j} \subseteq Y_{i',j'}$.

Let $i \geq 2$ and $1 \leq j \leq n_i$. Since $X_i \subseteq X_{i-1}$ and $Y_{i,j}$ is irreducible, there exists a j' with $1 \leq j' \leq n_{i-1}$ and $Y_{i,j} \subseteq Y_{i-1,j'}$. So we see that for every vertex on the i -level (i.e., for every vertex of the form (i, j)) there exists an arrow to a vertex on the $i - 1$ level. In particular, for every vertex there exists a path to the 1-level.

If $S_1 = \{Y_{i,j} \mid 1 \leq i \text{ and } 1 \leq j \leq n_i\}$ is finite, then also [\(14\)](#) is finite. So we suppose that S_1 is infinite. Since S_1 is infinite, there must exist a j_1 with $1 \leq j_1 \leq n_1$ such that

$$S_2 = \{Y_{i,j} \mid i \geq 2, 1 \leq j \leq n_i, \text{ there exists a path from } (i, j) \text{ to } (1, j_1)\}$$

is infinite. Set $Z_1 = Y_{1,j_1}$. Since S_2 is infinite, there exists a j_2 with $1 \leq j_2 \leq n_2$ such that $Y_{2,j_2} \in S_2$ and

$$S_3 = \{Y_{i,j} \mid i \geq 3, 1 \leq j \leq n_i, \text{ there exists a path from } (i, j) \text{ to } (2, j_2)\}$$

is infinite. Set $Z_2 = Y_{2,j_2}$. Then $Z_1 \supseteq Z_2$. Continuing like this, we obtain a descending chain $Z_1 \supseteq Z_2 \supseteq Z_3 \supseteq \dots$ of irreducible closed subsets of X and a descending chain $S_1 \supseteq S_2 \supseteq S_3 \supseteq \dots$ of infinite sets.

We claim that $Z_i = Z_{i+1}$ implies $S_i = S_{i+1}$. But if $Z_i = Z_{i+1}$, then there is exactly one arrow from level $i + 1$ to level i that points to (i, j_i) (because the representations $X_i = Y_{i,1} \cup \dots \cup Y_{i,n_i}$ are irredundant). So $S_i = S_{i+1}$.

By (i) we have $Z_i = Z_{i+1}$ for $i \gg 1$. Therefore $S_i = S_{i+1}$ for $i \gg 1$. But then S_i must consist of a single element for $i \gg 1$. This contradicts the fact that S_i is infinite.

Proposition 6.5. *Let R be a finitely σ -generated k - σ -algebra. Then the following two statements are equivalent:*

- (i) *Every ascending chain of radical well-mixed σ -ideals in R is finite.*
- (ii) *Every radical, well-mixed σ -ideal of R is the finite intersection of prime σ -ideals.*

Proof. We consider the set X of all prime σ -ideals of R as a topological space with respect to the topology induced from the Zariski topology on $\text{Spec}(R)$. Since every radical well-mixed σ -ideal $\mathfrak{a}$ of R is the intersection of the prime σ -ideals of R that contain $\mathfrak{a}$ ([Hru04, Lemma 2.10] or [Wib13, Prop. 1.2.28]), it follows that the map $\mathfrak{a} \mapsto V(\mathfrak{a}) = \{\mathfrak{p} \mid \mathfrak{a} \subseteq \mathfrak{p}\}$ from the set of radical well-mixed σ -ideals of R to the set of closed subsets of X is bijective. Moreover, for a radical, well-mixed σ -ideal $\mathfrak{a}$, the closed subset $V(\mathfrak{a})$ is irreducible if and only if $\mathfrak{a}$ is prime.

An ascending chain of radical well-mixed σ -ideals in R corresponds to a descending chain of closed subset of X . Thus, condition (i) translates to X being a Noetherian topological space. On the other hand, condition (ii) translates to: Every closed subset of X is a finite union of irreducible closed subsets.

It is known that every ascending chain of prime σ -ideals of R is finite ([Hru04, Lemma 4.34] or [Wib13, Cor. 5.1.6]). In other words, every descending chain of irreducible closed subsets of X is finite. Thus the claim follows from Lemma 6.4 $\square$

From Proposition 6.5 we immediately obtain:

Corollary 6.6. *Conjectures 6.1 and 6.2 are equivalent.*

6.2 Connected components

For the proof of Theorem 6.3 we need to introduce the group of connected components $\pi_0(G)$ of a σ -algebraic group G . We do not aim for an exhaustive study of $\pi_0(G)$ and the closely related notion of the identity component G° here. (The interested reader is referred to [Wib15, Section 4].) We rather work towards a proof of Theorem 6.3 as directly as possible.

An *irreducible (or connected) component* of a topological space is a maximal irreducible (or connected) subset. An irreducible (or connected) component is closed. Every topological space is the disjoint union of its connected components.

A *connected (or irreducible) component* of a σ -algebraic group G is a connected (or irreducible) component of $\text{Spec}(k\{G\})$. If R is a ring and $\mathfrak{a} \subseteq R$, we denote by $\mathcal{V}(\mathfrak{a})$ the closed subset of $\text{Spec}(R)$ defined by $\mathfrak{a}$. The following lemma is really about affine group scheme, rather than difference algebraic groups. But for lack of a suitable reference we include the proof.

Lemma 6.7. *Let G be a σ -algebraic group. The connected components and the irreducible components of G coincide. Moreover, if $\mathfrak{p}$ is a prime ideal of $k\{G\}$, then the connected component of G containing $\mathfrak{p}$ equals $\mathcal{V}(\mathfrak{a})$, where $\mathfrak{a}$ is the ideal of $k\{G\}$ generated by all idempotent elements of $k\{G\}$ contained in $\mathfrak{p}$.*

Proof. Let us fix a σ -closed embedding $G \hookrightarrow \mathcal{G}$ of G into some algebraic group $\mathcal{G}$ and for $i \geq 0$ let $G[i]$ denote the i -th order Zariski-closure of G in $\mathcal{G}$. Let $C \subseteq \text{Spec}(k\{G\})$ denote a connected component of G . Then $C = \mathcal{V}(\mathfrak{a})$ for a unique ideal $\mathfrak{a}$ of $k\{G\}$ generated by idempotent elements. (See [Sta19, Tag 00EB].) For every $i \geq 0$, the closure of the image of C

under the projection $\text{Spec}(k\{G\}) \rightarrow G[i]$ is connected and equal to $\mathcal{V}(\mathfrak{a} \cap k[G[i]]) \subseteq G[i]$. So $\mathcal{V}(\mathfrak{a} \cap k[G[i]]) \subseteq G[i]$ is contained in a connected component of $G[i]$. Assume that $G[i]$ has n_i connected components. Then

$$k[G[i]] = e_{i,1}k[G[i]] \oplus \cdots \oplus e_{i,n_i}k[G[i]]$$

for some primitive idempotent elements $e_{i,1}, \dots, e_{i,n_i} \in k[G[i]]$ and $\mathcal{V}(\mathfrak{a} \cap k[G[i]]) \subseteq \mathcal{V}(\mathfrak{b}_i)$ where $\mathfrak{b}_i = (e_{i,1}, \dots, e_{i,j_i-1}, e_{i,j_i+1}, \dots, e_{i,n_i}) \subseteq k[G[i]]$ for a unique $j_i \in \{1, \dots, n_i\}$. We have $\mathfrak{b}_{i+1} \cap k[G[i]] = \mathfrak{b}_i$ for $i \geq 0$ and $\mathfrak{b} := \bigcup_{i \geq 0} \mathfrak{b}_i$ is an ideal of $k\{G\}$. From $\mathcal{V}(\mathfrak{a} \cap k[G[i]]) \subseteq \mathcal{V}(\mathfrak{b}_i)$ it follows that $\mathfrak{b}_i$ is contained in the radical of $\mathfrak{a} \cap k[G[i]]$. Since the $e_{i,j}$'s are idempotent this shows that $\mathfrak{b}_i \subseteq \mathfrak{a}$. So $\mathfrak{b} \subseteq \mathfrak{a}$.

Since $k\{G\}/\mathfrak{b}$ may be interpreted as the directed union of the algebras $k[G[i]]/\mathfrak{b}_i \simeq e_{i,j_i}k[G[i]]$ which have a prime nilradical, it is clear that $\mathcal{V}(\mathfrak{b})$ is irreducible (and a fortiori connected). As $C = \mathcal{V}(\mathfrak{a}) \subseteq \mathcal{V}(\mathfrak{b})$ it follows from the maximality of C that $\mathcal{V}(\mathfrak{a}) = \mathcal{V}(\mathfrak{b})$. By the uniqueness of $\mathfrak{a}$ we have $\mathfrak{a} = \mathfrak{b}$.

We have thus shown that every connected component of G is irreducible. So the connected and the irreducible components of G coincide. The claimed form of the connected component of a prime ideal of $k\{G\}$ follows from the above arguments. $\square$

By Lemma 6.7, the connected components of a σ -algebraic group G are in bijection with the minimal prime ideals of $k\{G\}$. Contrary to the case of algebraic groups or differential algebraic groups, a difference algebraic group can have infinitely many components. Moreover, the components need not be open. This is illustrated in the following example.

Example 6.8. Let $G \leq \mathbb{G}_m$ be the σ -algebraic group given by

$$G(R) = \{g \in R^\times \mid g^2 = 1\} \leq \mathbb{G}_m(R)$$

for any k - σ -algebra R . We have

$$k\{G\} = k\{y\}/[y^2 - 1] = k[y, \sigma(y), \dots]/(y^2 - 1, \sigma(y)^2 - 1, \dots).$$

Let us assume that the characteristic of k is not equal to 2. Then the prime ideals of $k\{G\}$ are in bijection with the set of all sequences $(a_i)_{i \in \mathbb{N}}$ such that $a_i \in \{1, -1\}$. Every prime ideal of $k\{G\}$ is its own component. In particular, G has infinitely many components. The open subsets of $\text{Spec}(k\{G\})$ are all infinite, thus the components are not open.

For a σ -algebraic group G we define

$$\Sigma: \text{Spec}(k\{G\}) \rightarrow \text{Spec}(k\{G\}), \mathfrak{p} \mapsto \sigma^{-1}(\mathfrak{p}),$$

where $\sigma: k\{G\} \rightarrow k\{G\}$. A connected component C of G is *invariant* if $\Sigma(C) \subseteq C$.

Example 6.9. The σ -algebraic group from Example 6.8 has two invariant connected components, namely the prime ideals corresponding to the sequences $(1, 1, \dots)$ and $(-1, -1, \dots)$.

Lemma 6.10. *Let G be a σ -algebraic group and $C \subseteq \text{Spec}(k\{G\})$ a connected component of G . Then C is invariant if and only if C contains a prime σ -ideal.*

Proof. Assume first that C is invariant. By Lemma 6.7 the connected component C is of the form $C = \mathcal{V}(\mathfrak{p})$, for some prime ideal $\mathfrak{p}$ of $k\{G\}$. Since C is invariant, $\sigma^{-1}(\mathfrak{p}) \in \mathcal{V}(\mathfrak{p})$, i.e., $\mathfrak{p} \subseteq \sigma^{-1}(\mathfrak{p})$. Thus $\sigma(\mathfrak{p}) \subseteq \mathfrak{p}$ and $\mathfrak{p} \in C$ is a prime σ -ideal.

Conversely, assume that $\mathfrak{p} \in C$ is a prime σ -ideal. It follows from Lemma 6.7 that $C = \mathcal{V}(E)$, where E is the set of idempotent elements contained in $\mathfrak{p}$. Since $\sigma(\mathfrak{p}) \subseteq \mathfrak{p}$ we have $\sigma(E) \subseteq E$ and it follows that $\Sigma(C) \subseteq C$. $\square$

Corollary 6.11. *Let $k\{G\}$ be a k - σ -Hopf algebra that is finitely σ -generated over k . Then a minimal prime σ -ideal of $k\{G\}$ is a minimal prime ideal of $k\{G\}$.*

Proof. Let $\mathfrak{q} \subseteq k\{G\}$ be a minimal prime σ -ideal and let $C \subseteq \text{Spec}(k\{G\})$ be the connected component that contains $\mathfrak{q}$. Then $C = \mathcal{V}(\mathfrak{p})$ for a minimal prime ideal $\mathfrak{p}$ of $k\{G\}$. Since $\mathfrak{q} \in C$ it follows from Lemma 6.10 that C is invariant and so $\mathfrak{p}$ is a σ -ideal. Therefore $\mathfrak{q} = \mathfrak{p}$ by the minimality of $\mathfrak{q}$. $\square$

We will next introduce the group of connected components $\pi_0(G)$ of a σ -algebraic group G . This is a rather straight forward adaption of the standard construction for algebraic groups. See [Wat79, Sections 5 and 6] or [Mil17, Section 2.g]. We begin by defining appropriate analogs of étale algebras and étale algebraic groups.

Definition 6.12. *A finitely σ -generated k - σ -algebra R is σ -étale (over k) if R is integral over k and a separable k -algebra. A σ -algebraic group G is σ -étale if $k\{G\}$ is σ -étale over k .*

Thus, a finitely σ -generated k - σ -algebra R is σ -étale if and only if for every $r \in R$ there exists a separable polynomial f over k with $f(r) = 0$. Related notions of étaleness in difference algebra occur in [Tom14], [Tom16] and [TW18].

The σ -algebraic group from Example 2.14 is σ -étale. Moreover, if $\mathcal{G}$ is an étale algebraic group over k , then $[\sigma]_k \mathcal{G}$ is a σ -étale σ -algebraic group. σ -Étale σ -algebraic groups have a rather rigid structure which we will not discuss here. The interested reader is referred to Section 6 of [Wib15].

Recall ([Bou90, Chapter V, §6]) that a k -algebra A is étale if $A \otimes_k \bar{k}$ is a finite direct product of copies of $\bar{k}$, where $\bar{k}$ denotes the algebraic closure of k . For a k -algebra A we let $\pi_0(A)$ denote the union of all étale k -subalgebras of A . That is, $\pi_0(A)$ consists of all elements of A that annul a separable polynomial over k . Then $\pi_0(A)$ is a k -subalgebra of A . (Cf. Section 6.7 in [Wat79].)

Proposition 6.13. *Let G be a σ -algebraic group. There exists a σ -étale σ -algebraic group $\pi_0(G)$ and a morphism $G \rightarrow \pi_0(G)$ of σ -algebraic groups satisfying the following universal property: If $G \rightarrow H$ is a morphism of σ -algebraic groups with H σ -étale, then there exists a unique morphism $\pi_0(G) \rightarrow H$ such that*

$$\begin{array}{ccc} G & \xrightarrow{\quad} & \pi_0(G) \\ & \searrow & \swarrow \text{dotted} \\ & H & \end{array}$$

commutes.

Proof. The k -subalgebra $\pi_0(k\{G\})$ of $k\{G\}$ is a Hopf subalgebra. (Cf. Section 6.7 in [Wat79].) Let $a \in \pi_0(k\{G\})$ and let f be a separable polynomial over k with $f(a) = 0$. Let ${}^\sigma f$ denote the polynomial obtained from f by applying σ to the coefficients. Since $1 \in (f, f')$, it follows that also $1 \in ({}^\sigma f, ({}^\sigma f)')$. Thus ${}^\sigma f$ is separable. Since ${}^\sigma f(\sigma(a)) = 0$, we see that $\sigma(a) \in \pi_0(k\{G\})$. This shows that $\pi_0(k\{G\})$ is a k - σ -Hopf subalgebra of $k\{G\}$. Note that $\pi_0(k\{G\})$ is finitely σ -generated over k by Theorem 4.5. Let $\pi_0(G)$ denote the σ -étale σ -algebraic group represented by $\pi_0(k\{G\})$ and let $G \rightarrow \pi_0(G)$ be the morphism corresponding to the inclusion $\pi_0(k\{G\}) \subseteq k\{G\}$ (Remark 2.3).

If $G \rightarrow H$ is a morphism of σ -algebraic groups with H σ -étale, then the image of the dual map $k\{H\} \rightarrow k\{G\}$ consists of elements that annul a separable polynomial. Thus the image lies in $\pi_0(k\{G\})$ and $k\{H\} \rightarrow k\{G\}$ factors uniquely through $\pi_0(k\{G\}) \hookrightarrow k\{G\}$. $\square$

Of course $\pi_0(G)$ is unique up to a unique isomorphism.

Definition 6.14. Let G be a σ -algebraic group. The σ -étale σ -algebraic group $\pi_0(G)$ defined by the universal property of Proposition 6.13 is the group of connected components of G . The kernel G° of $G \rightarrow \pi_0(G)$ is the identity component of G .

The next lemma reduces the proof of Theorem 6.3 to σ -étale k - σ -algebras.

Lemma 6.15. Let G be a σ -algebraic group. There is a one-to-one correspondence between the connected components of G and the connected components of $\pi_0(G)$. Under this bijection invariant connected components correspond to invariant connected components. Moreover, every connected component of $\pi_0(G)$ is a single point.

Proof. Every prime ideal of $k\{\pi_0(G)\}$ is maximal and hence also minimal. This shows that the connected components of $\pi_0(G)$ are points. We identify $k\{\pi_0(G)\}$ with its image $\pi_0(k\{G\})$ in $k\{G\}$. We claim that $\mathfrak{p} \mapsto \mathfrak{p} \cap k\{\pi_0(G)\}$ is a bijection between the minimal prime ideals of $k\{G\}$ and the (minimal) prime ideals of $k\{\pi_0(G)\}$. Every (minimal) prime ideal of $k\{\pi_0(G)\}$ is of the form $\mathfrak{p} \cap k\{\pi_0(G)\}$ for some minimal prime ideal of $k\{G\}$ ([Bon72] Proposition 16, Chapter II, §2.6). On the other hand, if $\mathfrak{p}$ is a minimal prime ideal of $k\{G\}$, we see, using Lemma 6.7, that $\mathcal{V}(\mathfrak{p}) = \mathcal{V}(\mathfrak{a})$, where $\mathfrak{a}$ is the ideal of $k\{G\}$ generated by all idempotent elements of $k\{G\}$ contained in $\mathfrak{p}$. Thus $\mathfrak{p} = \sqrt{\mathfrak{a}}$. Since all idempotent elements of $k\{G\}$ lie in $k\{\pi_0(G)\}$, it follows that $(\mathfrak{a} \cap k\{\pi_0(G)\}) = \mathfrak{a}$. Therefore $\sqrt{(\mathfrak{p} \cap k\{\pi_0(G)\})} = \mathfrak{p}$.

If $\mathfrak{p}$ is a σ -ideal, then $\mathfrak{p} \cap k\{\pi_0(G)\}$ is a σ -ideal. Conversely, if $\mathfrak{p}' \subseteq k\{\pi_0(G)\}$ is a σ -ideal, then $\sqrt{(\mathfrak{p}')} \subseteq k\{G\}$ is a σ -ideal. $\square$

To show that a σ -algebraic group has only finitely many invariant connected components it thus suffices to show that any σ -étale σ -algebraic group has only finitely many invariant components. The latter statement holds indeed more generally:

Lemma 6.16. Let R be a finitely σ -generated k - σ -algebra. If R is σ -étale, then R has only finitely many prime σ -ideals.

Proof. Since R is σ -étale, every prime ideal of R is maximal and hence also minimal. If $\mathfrak{p}$ is a prime σ -ideal of R , then $\mathfrak{p} \subseteq \sigma^{-1}(\mathfrak{p})$ and therefore $\mathfrak{p} = \sigma^{-1}(\mathfrak{p})$. So every prime σ -ideal of R is reflexive. It follows from the Ritt-Raudenbush basis theorem (cf. Theorems 2.5.11 and 2.5.7 in [Lev08]) that a finitely σ -generated k - σ -algebra has only finitely many minimal reflexive prime

σ -ideals. Since every prime σ -ideal of R is a minimal reflexive prime σ -ideal of R , this implies that R has only finitely many prime σ -ideals. $\square$

The main results of this section now follow from the above considerations:

Theorem 6.17. *A σ -algebraic group has only finitely many invariant connected components.*

Proof. Let G be a σ -algebraic group. By Lemma 6.15, the invariant connected components of G are in bijection with the invariant connected components of $\pi_0(G)$. By Lemma 6.16 the σ -algebraic group $\pi_0(G)$ has only finitely many invariant connected components. $\square$

Proof of Theorem 6.3. By assumption $R = k\{G\}$ for a σ -algebraic group G . By Corollary 6.11 the set of minimal prime σ -ideals of $k\{G\}$ equals the set of minimal prime ideals of $k\{G\}$ that are σ -ideals. The latter set is finite by Theorem 6.17. $\square$

7 Difference algebraic relations among solutions of linear differential equations

Difference algebraic relations among solutions of differential equations are ubiquitous in the theory of special functions. A typical example is the recurrence relation

$$xJ_{\alpha+2}(x) - 2(\alpha+1)J_{\alpha+1}(x) + xJ_{\alpha}(x) = 0$$

satisfied by the Bessel function $J_{\alpha}(x)$. A Galois theoretic framework to analyze these relations has been developed in [DVHW14] and [DVHW17]. The Galois groups in this Galois theory are difference algebraic groups.

Combing this Galois theoretic approach with our Theorem 4.1, we show that the difference ideal of all difference algebraic relations among the solutions of a linear differential equations is finitely generated.

7.1 Difference algebras of finite presentation

Before discussing differential equations and the relations among their solutions, we establish some preparatory results concerning difference algebras of finite presentation. It appears that the notion of a finitely presented difference algebra does not occur in the difference algebra literature. The results we shall need are a rather direct analog of standard results about algebras of finite presentation. However, a crucial difference to note is that, while a finitely generated algebra over a field is automatically finitely presented, a finitely σ -generated difference algebra over a difference field need not be finitely σ -presented.

As before, k always denotes a σ -field.

Definition 7.1. *A k - σ -algebra R is finitely σ -presented if it is isomorphic to a quotient of a σ -polynomial ring over k modulo a finitely σ -generated σ -ideal. That is, $R \simeq k\{y_1, \dots, y_n\}/[f_1, \dots, f_m]$.*

Note that, using Definition 7.1, Theorem 4.1 can be restated as: The coordinate ring $k\{G\}$ of a σ -algebraic group G is finitely σ -presented.

Lemma 7.2. *Let $\psi: k\{z_1, \dots, z_\ell\} \rightarrow R$ be a surjective morphism of k - σ -algebras from a σ -polynomial ring over k onto R . If R is finitely σ -presented, then the kernel of ψ is a finitely σ -generated σ -ideal.*

Proof. We identify R with $k\{y_1, \dots, y_n\}/[f_1, \dots, f_m]$. Choose $g_i \in k\{y\}$ such that $\psi(z_i) = \overline{g_i}$ for $i = 1, \dots, \ell$. Then R is isomorphic to $k\{z, y\}/[z_i - g_i, f_j]$ via $\overline{y_j} \mapsto \overline{y_j}$. The inverse map is given by $\overline{z_i} \mapsto \overline{g_i}$, $\overline{y_j} \mapsto \overline{y_j}$.

Choose $h_j \in k\{z\}$ such that $\psi(h_j) = \overline{y_j}$ for $j = 1, \dots, n$ and consider the map $\varphi: k\{z, y\} \rightarrow k\{z\}$, $z_i \mapsto z_i$, $y_j \mapsto h_j$. Then $\psi \circ \varphi$ is $k\{z, y\} \rightarrow R$, $z_i \mapsto \overline{g_i}$, $y_j \mapsto \overline{y_j}$. As the kernel of $\psi \circ \varphi$ is $[z_i - g_i, f_j]$, it follows that the kernel of ψ is σ -generated by $\varphi(z_i - g_i), \varphi(f_j)$. $\square$

Lemma 7.3. *Let R be a k - σ -algebra and k'/k a σ -field extension. Then R is a finitely σ -presented k - σ -algebra if and only if $R \otimes_k k'$ is a finitely σ -presented k' - σ -algebra.*

Proof. Clearly $R \otimes_k k'$ is finitely σ -presented if R is. So let us assume that $R \otimes_k k'$ is a finitely σ -presented k' - σ -algebra. Then $R \otimes_k k'$ is finitely σ -generated over k' and we may choose a finite set of σ -generators from $R \subseteq R \otimes_k k'$. Let $\psi: k\{y\} \rightarrow R$ be the corresponding morphism of k - σ -algebras. Because the base change $\psi \otimes_k k': k'\{y\} \rightarrow R \otimes_k k'$ is surjective, also ψ must be surjective.

As $R \otimes_k k'$ is a finitely σ -presented k' - σ -algebra, it follows from Lemma 7.2 that $\ker(\psi \otimes_k k') \subseteq R \otimes_k k'$ is finitely σ -generated. As $\ker(\psi \otimes_k k') = \ker(\psi) \otimes_k k'$ we can indeed find a finite set $F \subseteq \ker(\psi)$ that σ -generates $\ker(\psi \otimes_k k')$. Then

$$[F] \otimes_k k' = \ker(\psi \otimes_k k') = \ker(\psi) \otimes_k k'.$$

Therefore $\ker(\psi) = [F]$ is finitely σ -generated and it follows that R is finitely σ -presented. $\square$

7.2 Difference Galois theory of differential equations

We briefly recall some of the basic notions from [DVHW14]. A $\delta\sigma$ -field is a field K together with a derivation $\delta: K \rightarrow K$ and an endomorphism $\sigma: K \rightarrow K$ such that δ and σ commute up to a factor annulled by the derivation. We will always assume that K is a $\delta\sigma$ -field of characteristic zero. A typical example, matching up with the example of the Bessel's function given above, is $K = \mathbb{C}(\alpha, x)$ with $\delta = \frac{\partial}{\partial x}$ and $\sigma(f(\alpha, x)) = f(\alpha + 1, x)$. Note that for a $\delta\sigma$ -field K , the field $k = K^\delta = \{a \in K \mid \delta(a) = 0\}$ is a σ -field.

A σ -Picard-Vessiot extension for $\delta(y) = Ay$, where $A \in K^{n \times n}$, is a $\delta\sigma$ -field extension L/K such that

- there exists $Y \in \text{GL}_n(L)$ with $\delta(Y) = AY$ such that L is σ -generated by the entries of Y as a σ -field extension of K and
- $L^\delta = K^\delta$.

Note that the K - σ -algebra $S = K\{Y, \frac{1}{\det(Y)}\}$, called a σ -Picard-Vessiot ring for $\delta(y) = Ay$, is also stable under the derivation δ . It encodes the difference algebraic relations among the solutions of $\delta(y) = Ay$: If Z is an $n \times n$ -matrix of σ -indeterminates over K , then the kernel $\mathfrak{a}$ of $K\{Z, \frac{1}{\det(Z)}\} \rightarrow S$, $Z \mapsto Y$ is the difference ideal of all difference algebraic relations among the entries of Y and $K\{Z, \frac{1}{\det(Z)}\}/\mathfrak{a} \simeq S$.

The σ -Galois group G of L/K is the functor from k - σ -Alg to Groups that associates to every k - σ -algebra R , the group of $\delta\sigma$ -automorphism of $S \otimes_k R$ over $K \otimes_k R$. (The derivation δ on R is assumed to be trivial.) It is shown in [DVHW14, Prop. 2.5] that G is a σ -algebraic group. It measures the difference algebraic relations among the entries of Y . We are now prepared to prove the main result of this section:

Theorem 7.4. *Let L/K be a σ -Picard-Vessiot extension for $\delta(y) = Ay$ and $Y \in \mathrm{GL}_n(L)$ such that $\delta(Y) = AY$. Then the kernel of $K\{Z, \frac{1}{\det(Z)}\} \rightarrow L$, $Z \mapsto Y$ is a finitely σ -generated σ -ideal.*

Proof. Let z be a further σ -variable. If the kernel of $K\{Z, z\} \rightarrow L$, $Z \mapsto Y$, $z \mapsto \frac{1}{\det(Y)}$ is finitely σ -generated, also the kernel of $K\{Z, \frac{1}{\det(Z)}\} \rightarrow L$, $Z \mapsto Y$ is finitely σ -generated. Therefore, by Lemma 7.2, it suffices to show that the σ -Picard-Vessiot ring $S = K\{Y, \frac{1}{\det(Y)}\}$ is a finitely σ -presented K - σ -algebra. The algebraic recast of the torsor theorem ([DVHW14, Lemma 2.7]) tells us that $S \otimes_K S \simeq S \otimes_k k\{G\}$, where G is the σ -Galois group of L/K .

This isomorphism extends to $L \otimes_K S \simeq L \otimes_k k\{G\}$. By Theorem 4.1 the coordinate ring $k\{G\}$ is a finitely σ -presented k - σ -algebra. Therefore $L \otimes_k k\{G\} \simeq L \otimes_K S$ is a finitely σ -presented L - σ -algebra. It thus follows from Lemma 7.3 that S is a finitely σ -presented K - σ -algebra. $\square$

References

- [Bou72] Nicolas Bourbaki. *Elements of mathematics. Commutative algebra*. Hermann, Paris, 1972. Translated from the French.
- [Bou90] N. Bourbaki. *Algebra. II. Chapters 4–7*. Elements of Mathematics (Berlin). Springer-Verlag, Berlin, 1990. Translated from the French by P. M. Cohn and J. Howie.
- [Bou02] Élisabeth Bouscaren. Théorie des modèles et conjecture de Manin-Mumford (d’après Ehud Hrushovski). *Astérisque*, (276):137–159, 2002. Séminaire Bourbaki, Vol. 1999/2000.
- [Bui92] Alexandru Buium. *Differential algebraic groups of finite dimension*, volume 1506 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1992.
- [Bui93] Alexandru Buium. Geometry of differential polynomial functions. I. Algebraic groups. *Amer. J. Math.*, 115(6):1385–1444, 1993.
- [Bui98] Alexandru Buium. Differential subgroups of simple algebraic groups over p -adic fields. *Amer. J. Math.*, 120(6):1277–1287, 1998.
- [BW] Annette Bachmayr and Michael Wibmer. Torsors for difference algebraic groups. arXiv:1607.07035.
- [Cas72] Phyllis J. Cassidy. Differential algebraic groups. *Amer. J. Math.*, 94:891–954, 1972.
- [Cas75] Phyllis Joan Cassidy. The differential rational representation algebra on a linear differential algebraic group. *J. Algebra*, 37(2):223–238, 1975.

- [Cas78] Phyllis J. Cassidy. Unipotent differential algebraic groups. In *Contributions to algebra (collection of papers dedicated to Ellis Kolchin)*, volume 51 of *Astérisque*, pages 83–115. Soc. Math. France, Paris, 1978.
- [Cas89] Phyllis Joan Cassidy. The classification of the semisimple differential algebraic groups and the linear semisimple differential algebraic Lie algebras. *J. Algebra*, 121(1):169–238, 1989.
- [CH99] Zoé Chatzidakis and Ehud Hrushovski. Model theory of difference fields. *Trans. Amer. Math. Soc.*, 351(8):2997–3071, 1999.
- [CH17] Zoé Chatzidakis and Ehud Hrushovski. On subgroups of semi-abelian varieties defined by difference equations. *Trans. Amer. Math. Soc.*, 369(5):3673–3705, 2017.
- [Cha97] Zoé Chatzidakis. Groups definable in ACFA. In *Algebraic model theory (Toronto, ON, 1996)*, volume 496 of *NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci.*, pages 25–52. Kluwer Acad. Publ., Dordrecht, 1997.
- [Cha01] Zoé Chatzidakis. Difference fields: model theory and applications to number theory. In *European Congress of Mathematics, Vol. I (Barcelona, 2000)*, volume 201 of *Progr. Math.*, pages 275–287. Birkhäuser, Basel, 2001.
- [CHP02] Zoé Chatzidakis, Ehud Hrushovski, and Ya’acov Peterzil. Model theory of difference fields. II. Periodic ideals and the trichotomy in all characteristics. *Proc. London Math. Soc. (3)*, 85(2):257–311, 2002.
- [CK18] Marcin Chalupnik and Piotr Kowalski. Difference modules and difference cohomology. *Algebra Number Theory*, 12(7):1559–1580, 2018.
- [Coh65] Richard M. Cohn. *Difference algebra*. Interscience Publishers John Wiley & Sons, New York-London-Sydney, 1965.
- [CP] Zoé Chatzidakis and Anand Pillay. Generalized Picard-Vessiot extensions and differential Galois cohomology. *arXiv:1702.01969*.
- [CS07] Phyllis J. Cassidy and Michael F. Singer. Galois theory of parameterized differential equations and linear differential algebraic groups. In *Differential equations and quantum groups*, volume 9 of *IRMA Lect. Math. Theor. Phys.*, pages 113–155. Eur. Math. Soc., Zürich, 2007.
- [CS11] Phyllis J. Cassidy and Michael F. Singer. A Jordan-Hölder theorem for differential algebraic groups. *J. Algebra*, 328:190–217, 2011.
- [DG70] Michel Demazure and Pierre Gabriel. *Groupes algébriques. Tome I: Géométrie algébrique, généralités, groupes commutatifs*. Masson & Cie, Éditeur, Paris; North-Holland Publishing Co., Amsterdam, 1970. Avec un appendice it Corps de classes local par Michiel Hazewinkel.
- [DVHW14] Lucia Di Vizio, Charlotte Hardouin, and Michael Wibmer. Difference Galois theory of linear differential equations. *Adv. Math.*, 260:1–58, 2014.

- [DVHW17] Lucia Di Vizio, Charlotte Hardouin, and Michael Wibmer. Difference algebraic relations among solutions of linear differential equations. *J. Inst. Math. Jussieu*, 16(1):59–119, 2017.
- [Fre15] James Freitag. Indecomposability for differential algebraic groups. *J. Pure Appl. Algebra*, 219(7):3009–3029, 2015.
- [GO14] Sergey Gorchinskiy and Alexey Ovchinnikov. Isomonodromic differential equations and differential categories. *J. Math. Pures Appl. (9)*, 102(1):48–78, 2014.
- [Gro70] *Schémas en groupes. I: Propriétés générales des schémas en groupes*. Séminaire de Géométrie Algébrique du Bois Marie 1962/64 (SGA 3). Dirigé par M. Demazure et A. Grothendieck. Lecture Notes in Mathematics, Vol. 151. Springer-Verlag, Berlin, 1970.
- [HMO17] Charlotte Hardouin, Andrei Minchenko, and Alexey Ovchinnikov. Calculating differential Galois groups of parametrized differential equations, with applications to hypertranscendence. *Math. Ann.*, 368(1-2):587–632, 2017.
- [Hru01] Ehud Hrushovski. The Manin-Mumford conjecture and the model theory of difference fields. *Ann. Pure Appl. Logic*, 112(1):43–115, 2001.
- [Hru04] Ehud Hrushovski. The elementary theory of the Frobenius automorphisms, 2004. arXiv:math/0406514v1, updated version available from <http://www.ma.huji.ac.il/~ehud/>, references in the text are to the updated version.
- [HS08] Charlotte Hardouin and Michael F. Singer. Differential Galois theory of linear difference equations. *Math. Ann.*, 342(2):333–377, 2008.
- [Jan87] Jens Carsten Jantzen. *Representations of algebraic groups*, volume 131 of *Pure and Applied Mathematics*. Academic Press Inc., Boston, MA, 1987.
- [Kam13] Moshe Kamensky. Tannakian formalism over fields with operators. *Int. Math. Res. Not. IMRN*, 24:5571–5622, 2013.
- [Kol85] E. R. Kolchin. *Differential algebraic groups*, volume 114 of *Pure and Applied Mathematics*. Academic Press Inc., Orlando, FL, 1985.
- [KP00] Piotr Kowalski and Anand Pillay. Pro-algebraic and differential algebraic group structures on affine spaces. *Amer. J. Math.*, 122(1):213–221, 2000.
- [KP02] Piotr Kowalski and A. Pillay. A note on groups definable in difference fields. *Proc. Amer. Math. Soc.*, 130(1):205–212 (electronic), 2002.
- [KP07] Piotr Kowalski and Anand Pillay. On algebraic σ -groups. *Trans. Amer. Math. Soc.*, 359(3):1325–1337 (electronic), 2007.
- [Lan08] Peter Landesman. Generalized differential Galois theory. *Trans. Amer. Math. Soc.*, 360(8):4441–4495, 2008.

- [Lev08] Alexander Levin. *Difference algebra*, volume 8 of *Algebra and Applications*. Springer, New York, 2008.
- [Lev15] Alexander Levin. On the ascending chain condition for mixed difference ideals. *Int. Math. Res. Not. IMRN*, (10):2830–2840, 2015.
- [Mac97] Angus Macintyre. Generic automorphisms of fields. *Ann. Pure Appl. Logic*, 88(2-3):165–180, 1997. Joint AILA-KGS Model Theory Meeting (Florence, 1995).
- [Mal10] B. Malgrange. Differential algebraic groups. In *Algebraic approach to differential equations*, pages 292–312. World Sci. Publ., Hackensack, NJ, 2010.
- [Mil17] J. S. Milne. *Algebraic groups*, volume 170 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2017. The theory of group schemes of finite type over a field.
- [Min15] Andrey Minchenko. On central extensions of simple differential algebraic groups. *Proc. Amer. Math. Soc.*, 143(6):2317–2330, 2015.
- [MO11] Andrey Minchenko and Alexey Ovchinnikov. Zariski closures of reductive linear differential algebraic groups. *Adv. Math.*, 227(3):1195–1224, 2011.
- [MO13] Andrey Minchenko and Alexey Ovchinnikov. Extensions of differential representations of $\mathbf{SL}_2$ and tori. *J. Inst. Math. Jussieu*, 12(1):199–224, 2013.
- [MO19] Andrei Minchenko and Alexey Ovchinnikov. Triviality of differential Galois cohomology of linear differential algebraic groups. *Communications in Algebra*, 2019. <https://doi.org/10.1080/00927872.2019.1612416>
- [MOS14] Andrey Minchenko, Alexey Ovchinnikov, and Michael F. Singer. Unipotent differential algebraic groups as parameterized differential Galois groups. *J. Inst. Math. Jussieu*, 13(4):671–700, 2014.
- [MOS15] Andrey Minchenko, Alexey Ovchinnikov, and Michael F. Singer. Reductive linear differential algebraic groups and the Galois groups of parameterized linear differential equations. *Int. Math. Res. Not. IMRN*, (7):1733–1793, 2015.
- [MS11] Rahim Moosa and Thomas Scanlon. Generalized Hasse-Schmidt varieties and their jet spaces. *Proc. Lond. Math. Soc. (3)*, 103(2):197–234, 2011.
- [Ovc09] Alexey Ovchinnikov. Differential Tannakian categories. *J. Algebra*, 321(10):3043–3062, 2009.
- [OW15] Alexey Ovchinnikov and Michael Wibmer. σ -Galois theory of linear difference equations. *Int. Math. Res. Not. IMRN*, (12):3962–4018, 2015.
- [OW17] Alexey Ovchinnikov and Michael Wibmer. Tannakian categories with semigroup actions. *Canad. J. Math.*, 69(3):687–720, 2017.
- [Pil97] Anand Pillay. Some foundational questions concerning differential algebraic groups. *Pacific J. Math.*, 179(1):179–200, 1997.

- [Pil98] Anand Pillay. Differential Galois theory. I. *Illinois J. Math.*, 42(4):678–699, 1998.
- [Pil17] Anand Pillay. The Picard-Vessiot theory, constrained cohomology, and linear differential algebraic groups. *J. Math. Pures Appl. (9)*, 108(6):809–817, 2017.
- [RR39] J. F. Ritt and H. W. Raudenbush, Jr. Ideal theory and algebraic difference equations. *Trans. Amer. Math. Soc.*, 46:445–452, 1939.
- [Sca05] Thomas Scanlon. A positive characteristic Manin-Mumford theorem. *Compos. Math.*, 141(6):1351–1364, 2005.
- [Sca06] Thomas Scanlon. Local André-Oort conjecture for the universal abelian variety. *Invent. Math.*, 163(1):191–211, 2006.
- [Sit74] William Yu Sit. Typical differential dimension of the intersection of linear differential algebraic groups. *J. Algebra*, 32(3):476–487, 1974.
- [Sit75] William Yu Sit. Differential algebraic subgroups of $SL(2)$ and strong normality in simple extensions. *Amer. J. Math.*, 97(3):627–698, 1975.
- [Sta19] The Stacks Project Authors. Stacks Project. <http://stacks.math.columbia.edu>, 2019.
- [SV99] Thomas Scanlon and José Felipe Voloch. Difference algebraic subgroups of commutative algebraic groups over finite fields. *Manuscripta Math.*, 99(3):329–339, 1999.
- [Tak72] Mitsuhiro Takeuchi. A correspondence between Hopf ideals and sub-Hopf algebras. *Manuscripta Math.*, 7:251–270, 1972.
- [Tom14] Ivan Tomašić. A twisted theorem of Chebotarev. *Proc. Lond. Math. Soc.*, 108(2):291–326, 2014.
- [Tom16] Ivan Tomašić. Twisted Galois stratification. *Nagoya Math. J.*, 222(1):1–60, 2016.
- [TW18] Ivan Tomašić and Michael Wibmer. Strongly étale difference algebras and Babbitt’s decomposition. *J. Algebra*, 504:10–38, 2018.
- [Wan17] Jie Wang. Monomial difference ideals. *Proc. Amer. Math. Soc.*, 145(4):1481–1496, 2017.
- [Wan18] Jie Wang. Finite basis for radical well-mixed difference ideals generated by binomials. *Comm. Algebra*, 46(6):2589–2599, 2018.
- [Wat79] William C. Waterhouse. *Introduction to affine group schemes*, volume 66 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1979.
- [Wib13] Michael Wibmer. Algebraic difference equations, 2013. Lecture notes, <http://www.math.tugraz.at/~wibmer/ADE.pdf>.
- [Wib15] Michael Wibmer. Affine difference algebraic groups, 2015. Habilitation thesis, RWTH Aachen University, 146 pages, <http://www.math.tugraz.at/~wibmer/habil.pdf>.